SERVICE DESCRIPTION

TeleSec OneTimePass

Deutsche Telekom Security GmbH

Version	5.3
Last revised	24.11.2020

LIFE IS FOR SHARING.

Publication details

PUBLISHED BY

DEUTSCHE TELEKOM SECURITY GMBH
Bonner Talweg 100
53113 Bonn

Phone: +49 228 181-0 | E-mail: info@telekom.de | Internet: www.telekom.de/security
Supervisory Board: Adel Al-Saleh (chairman) | Management Board: Thomas Fetten (spokesman), Dr. Klaus Schmitz, Thomas Tschersich
Trade Register: District Court Bonn HRB 15241, Registered Office Bonn | Tax ID No. DE 254595345 | WEEE-Reg.-No. DE 56768674

Contents

1 Preamble

OneTimePass enables user identification in a network or on the Internet.

It offers a strong 2-factor-authentication based on dynamic one-time passwords.

The service generates one-time passwords for a login to online services and secured systems and offers its own user administration.

The customer can choose between different token types.

TeleSec OneTimePass is operated in the high-secured and certified Deutsche Telekom Trust Center.

2 Services provided by Telekom Security

The services provided by Telekom Security is divided into different calling plans, the operation and specification of the service, as well as the functions and different kinds of authentication media ("token").

2.1 Provision of services – Calling Plans

Various rate models are available to the customer for the OneTimePass service:

2.1.1 OneTimePass Trial Period

A service that is not restricted by the scope of delivery. There are no monthly costs. Only a one-time provision fee is invoiced for the trial period and includes two OTP Reader III, two Smart Card NetKey 3.0 and five OneTimePass Tokens. The trial period lasts maximally 8 weeks (or per agreement). If a service is ordered after expiration of the trial period, the provision price will be settled with the corresponding provision price of the rate.

2.1.2 OneTimePass Compact

A service that is restricted by the scope of delivery. Only one OneTimePass group (see item 1.2.3) is available and only a limited number of users can be set up. The administration rights and services through the service websites are also restricted. Only the administrator function is available. The rate model is invoiced monthly at a flat rate and is independent of the number of users and the number of authentications. Service provision includes delivery of two OTP Reader III and two Smart Card NetKey 3.0 for administrators. This model is suitable for up to 100 users. The Compact rate model offers the following levels/packages:

<u>Compact 10, 25, 50 or 75</u>
With OneTimePass Compact 10/25/50/75, one OneTimePass Group having up to 10/25/50/75 users shall be set up for the customer.

<u>Upgrade</u>
Telekom Security shall carry out upgrades from a lower OneTimePass level (Compact 25 or Compact 50) to a higher OneTimePass level (Compact 50 or Compact 75).

<u>Increase in the number of OneTimePass (Compact 75) users</u>
Telekom Security shall increase the number of OneTimePass (Compact 75) users in increments of 50 or 100 additional users, respectively.

2.1.3 OneTimePass Advanced

This rate model is not restricted by the scope of delivery. A monthly flat fee will be invoiced for the provision of this service. OneTimePass users will also be invoiced a monthly flat fee and are independent of the number of authentications. The provision of the service includes the delivery of two OTP Reader III and two SmartCard NetKey 3.0 for administrators. This model is suitable for any desired amount of users. The Advanced rate model distinguishes between the following levels or packages:

Advanced 100, ... License

With OneTimePass (Advanced 100, 250, 500, 1,000, 2,500, 5,000, 7,500, 10,000 and 10,000+) the number of users is restricted for the customer according to the packages irrespective of the number of OneTimePass user groups in which the OneTimePass user is being administered. The price levels can be changed by upgrades or downgrades.

Advanced Extension 50, ... License

With OneTimePass (Advanced Extension 50, 100, 500 and 1,000) smaller jumps in levels can be made. For example, OneTimePass Advanced 1,000 (= 1,000 users) can be expanded by a OneTimePass Advanced Extension 500 (= 500 users) to a total of 1,500 users. The Advanced Extension packages remain in the inventory until cancellation and are not settled with an upgrade or downgrade of OneTimePass Advanced. So if, in the above example, OneTimePass Advanced 1,000 is increased to OneTimePass Advanced 2,500, Extension 500 will remain in existence unless it is cancelled. This means that 3,000 users are now available.

The volume of an Advanced Extension may not be larger than the volume of the commissioned Advanced package. The Advanced Extensions 500 and 1,000 may not therefore be used for Advanced 100 and 250.

2.1.4 OneTimePass Reseller

This rate model is not restricted by the scope of delivery and is only available to specified partners of Deutsche Telekom.

2.2 Operation – OneTimePass service

The central identification service is operated by Deutsche Telekom in its Trust Center and provided to the provider for the agreed contract term.

With the OneTimePass authentication media, a user can access an Internet server or a local network (e.g., an Internet service provider) using a one-time password. The authentication media can also be used to authenticate transactions (replacing the PIN/TAN) and to authenticate customers of a customer service hotline. In the query field of the remote data transfer network/Internet browser, the user enters the ID number or alias name that is printed on the smart card and the one-time password that is generated by the smart card or the token and shown on the card reader display. On the push of a button (token) or after the smart card has been inserted in the reader and the PIN has been entered, the password will always be recalculated and will be valid only once. The server that is protected by OneTimePass submits an electronic validity request (standard remote authentication dial-in user service pursuant to protocol RFC 2865 and RFC 2868 – RADIUS –) via the Internet to the OneTimePass server in T-System’s Trust Center. This server will check the validity of the OneTimePass and return the attributes set for the corresponding user or group profile. The Telekom Security Trust Center will not associate the request with an actual person; only the card identification number or the alias name will be known.

2.2.1 OneTimePass server

In its Trust Center, Telekom Security operates a central OneTimePass server that checks the validity of the one-time passwords submitted by the OneTimePass provider. A RADIUS server (RFC 2865 and RFC 2868) will be used to connect the OneTimePass server to the Internet. All providers will be administered in the central server. Each provider can administer individual groups and profiles. Due to this central administration, the OneTimePass tokens (see 1.1) can be used for different applications by different providers if they have been activated by the respective provider.

2.2.2 OneTimePass group

The OneTimePass provider can assign users to so-called user groups in order to differentiate and identify them according to applications and customer groups/departments (accounting, street worker, etc.) All users in a group can be assigned the same RADIUS attributes if desired. This will simplify the administration of individual users. The OneTimePass provider can set up a restriction of the OneTimePass for the OneTimePass users. Depending on the price model or package, the number of OneTimePass groups can be limited by Telekom Security (only for OneTimerPass Compact – there is a limitation to one group per customer).

2.2.3 Provider’s General Supervisor

For the administration of the OneTimePass, each provider shall receive General Supervisor authorizations. Each General Supervisor will receive a OneTimePass medium for identification on the Trust Center Internet service pages. The authorizations or services are described in section 1.2.8.1.

2.2.4 OneTimePass user

The OneTimePass user is identified by the OneTimePass provider and has a OneTimePass authentication medium assigned to them. Users are administered via the Internet service pages of the Trust Center. The authorizations or services are described in section 1.2.8.1. Depending on the price model or package, the number of OneTimePass users can be limited by Telekom Security.

2.2.5 RADIUS - User Profile

Telekom Security provides OneTimePass providers with RADIUS attributes in accordance with RFC 2865 and RFC 2886. These attributes can be assigned to a OneTimePass group or a OneTimePass user. They are administered via the Internet service pages of the Telekom Security Trust Center.

2.2.6 RADIUS – Rules

The OneTimePass platform supports the creation of sets of rules that enable the user to define for a certain group the conditions (input attributes) subject to which various actions (output attributes) can be performed. Collectively, the conditions and actions are referred to as events. Administration is done through the Internet service page for administrators.

2.2.7 RADIUS – IP Pool (Dynamic IP Address Allocation)

IP pools can be used to define IP address areas, which can be assigned to the *Framed-IP-Address* group or user attribute. During a RADIUS query, an IP address from this pool that has not yet been assigned is assigned to the user. Thanks to RADIUS accounting functions, the OneTimePass RADIUS server can independently administer these dynamic IP address pools. IP pools are defined through a network screen, a start address and an end address, and are identified through a name that is unique in the group. Administration is done through the Internet service page for administrators.

The following rules apply to the definition of IP pools:

- A maximum of 5 IP pools can be created per group.
- Since the name of the pool is used as the value of an attribute, the same restrictions apply to special characters as to attribute values.
- The subnet mask is indicated in the CIDR notation (for example, 111.222.1.0/24)
- A pool may maximally contain an address interval of 4,096 values. This means that the value for the network suffix may not be smaller than 20.

2.2.8 One-time password check

The one-time password shall be generated with the OneTimePass authentication token (smart card reader and smart card). With the OneTimePass Token, a new one-time password is generated with the push of a button and is sent to the RADIUS server along with the server PIN for verification. With the smart card reader and smart card, the OneTimePass user is prompted to enter their PIN after inserting the smart card into the smart card reader. After the PIN has been entered and confirmed with the enter key, the smart card reader generates an eight-digit numeric one-time password. After the username and one-time password has been entered into the query dialog box (e.g., remote data transfer connection), the connection to the OneTimePass provider is established. The Internet is primarily used as the transmission medium.

No access to the client software or hardware is required to participate in the OneTimePass service.

The OneTimePass user's request is first routed to the provider's standard RADIUS server. The RADIUS protocol enables user identification by means of saved data in a local or external database. The RADIUS server receives a special profile in order to be able to use the OneTimePass service. This profile suppresses the authentication request to the internal database and automatically establishes a connection to the Telekom Security Trust Center. Other components that support the RADIUS protocol may also be used instead of a RADIUS server.

In order to be able to use the OneTimePass standard service, the provider usually only needs the existing infrastructure, e.g., a router, the RADIUS protocol, a user database with the user profile and access to the Trust Center via the Internet.

For the password check, the OneTimePass provider shall transfer only the card number or the alias name and the current one-time password and –if applicable- the server-PIN (8- or 12-digits) to the Telekom Security Trust Center via the RADIUS protocol. The OneTimePass feature, consisting of an individual DES-3 key and an initialization vector (starting value for the first valid password) is saved to the card for the generation of one-time passwords during smart card production. The central OneTimePass server at the Telekom Trust Center also knows this starting value and the mathematical algorithm for further password generation. With the help of this parameter, the Trust Center automatically generates another 15 passwords in advance. If the user now generates several passwords that he does not send to the Trust Center for verification, then synchronization can only be guaranteed within these boundaries. Each password shall be valid only once.

As soon as a one-time password has been used, all previously generated one-time passwords shall become invalid.

Moreover, the central server shall know whether the smart card is valid or has been barred. When the OneTimePass provider requests password verification, the date, time and card number or alias are saved in the database. After verification of the one-time password in the Telekom Security Trust Center the user receives a confirmation or a rejection.

The Telekom Security Trust Center shall have no knowledge of any personal or user data.

After the confirmation by the Telekom Security Trust Center, the user rights for the application are allocated to the OneTimePass user by the OneTimePass provider by means of RADIUS protocol. The OneTimePass user is activated for the application by the OneTimePass provider .

The OneTimePass service only comprises user identification. No encrypted connection is established.

An encrypted connection between a web server and a OneTimePass user can be established by means of an SSL or IPSEC connection, for example. A secure SSL connection is established by the TeleSec product ServerPass.

2.2.9 OneTimePass Administration

2.2.9.1 Internet service website - providers

Telekom Security runs an Internet server on which the OneTimePass provider can carry out all administrative tasks itself. Each access is encrypted by means of an SSL server certificate (TeleSec ServerPass). Authentication occurs via user ID/one-time password. The requisite one-time password is generated by means of the OneTimePass authentication media. The card reader OTP-Reader III (see section 1.1.1) in conjunction with the smart card (see section 1.1.3) is required as the standard authentication medium. Depending on your company's security policy, administrator/supervisor login can also be enabled through an OneTimePass Token or OneTimePass mobile (no longer provided). However, login using these authentication media must first be activated by the General Supervisor.

OneTimePass offers the following user authorizations for customer service and administration:

OneTimePass general supervisor:

- FAQs, contacts, recent messages, downloads
- Setup and maintain (change, block and delete) supervisors
- Set up and maintain OneTimePass groups
- Define user restrictions per OneTimePass group
- Blocking service for general supervisor and supervisor
- Set up and maintain RADIUS client groups
- Request new RADIUS clients
- Access monthly OTP provider statistics (reporting and statistical data)

OneTimePass supervisor:

- FAQs, contacts, recent messages, downloads
- Set up and maintain (change, bar, delete) administrators for the authorized OneTimePass groups
- Blocking service for administrators
- Allocation of standard RADIUS attributes to all administrators
- Allocation of special RADIUS attributes to individual administrators

The supervisor has the above authorizations for the OneTimePass providers assigned to him, along with their OneTimePass groups. For example, a supervisor may be responsible for multiple OneTimePass providers and all OneTimePass groups resulting therefrom.

OneTimePass administrator:

- FAQs, contacts, recent messages, downloads
- Service – status information on token or smart cards
- Set up and maintain (change, bar, delete, synchronize) users for the authorized OneTimePass groups
- Maintain RADIUS group attributes according to the supervisor's specifications
- Maintain special RADIUS user attributes according to the supervisor's specifications

The administrator has the above authorizations for the OneTimePass providers assigned to him, along with their OneTimePass groups. For example, an administrator may be responsible for multiple OneTimePass providers and all OneTimePass groups resulting therefrom.

2.2.9.2 SOAP administration

As an alternative to using the service websites, the complete OneTimePass administration can also be carried out on the basis of SOAP. All administrative activities were replicated in the form of specified SOAP requests . This means that an administration portal that already exists can be easily connected to OneTimePass. The authentication is done with the aid of a Shared Business CA certificate. The document “OneTimePass SOAP Specification Vn.pdf”, which is available as an alternative, contains the complete command set incl. WSDL description.

2.2.9.3 Bulk administration

For efficient simultaneous administration/management of many users, the functions for mass administration, snapshots and user exports are offered with bulk administration.

Mass Administration:
Mass administration enables mass creation, modification and deletion of up to 5,000 data records. Similarly to when you create users manually, an overview of the group attributes will first appear. These attributes are automatically assigned to each new user created, but can be individually assigned further definitions.
Data records can be transmitted in two ways: They can either be transferred as a file upload onto the sever, or alternatively they can be entered directly into the text field provided or copied from the clipboard. The method to be used is defined in the relevant selection field.

Alongside creating new users, the import function can also be used to modify existing users. Depending on the type of token, changes may affect the server PIN, the service password and the user attributes. This function can be managed by the selection box underneath the entry field. If this function is activated when data is transferred, all current available users will be modified without any further confirmation required. If attributes are provided for a user to be modified, all previously defined attributes will be deleted and only those values specified in the data record will be applied.

Data records are transferred in CSV format, using a semicolon as a delimiter.

Snapshots
The snapshots function is used to back up user data before mass administration is carried out. All information linked to the user, including the token number, alias and lock status, is backed up. All attributes assigned for the user are also backed up.

The “snapshots” service feature can be activated for each customer by the Trust Center administrators, if required.

User export
Another function in the *Bulk administration* area is the function for exporting user data. This function can be used to export all user data for the selected group to a file in the format that is needed for input data in the mass administration function. The export file created is offered to you for download in a second browser window.

2.2.9.4 Internet service website - users

Telekom Security shall operate an Internet server for the OneTimePass users on which all user-related tasks can be performed. All queries to this server shall be transmitted encoded with an SSL server certificate. Telekom Security offers the following services:

- Allocation of blocking passwords
- Synchronization of token or smart card
- Presentation of user profile
- Blocking service
- Frequently asked questions (FAQ)
- Statistics and overviews
- Download area (manuals, etc).

2.2.10 Blocking service

Since OneTimePass is a central service, the OneTimePass user can log in with several OneTimePass providers with the OneTimePass authentication medium without impairing their application or endangering their secure access. OneTimePass therefore differentiates between different blocking authorizations.

The possible reasons for blocking a card or token include:

- Defective smart card/defective token
- The operator error counter stops after the incorrect PIN has been entered several times; the card is useless
- The OneTimePass user has lost the smart card or token
- The smart card / token has been stolen
- OneTimePass is no longer used by the OneTimePass user
- The provider bars the OneTimePass user from certain user groups.

2.2.10.1 OneTimePass provider

The OneTimePass provider shall be entitled to bar all OneTimePass users within his user groups. This way the provider ensures that unauthorized users cannot access his data.

A provider shall not be entitled to bar a user globally since the OneTimePass user can use the authentication medium for identification with other providers.

Global blocking of the smart card can only be initiated by the OneTimePass user. Blocks become effective as soon as they have been activated in the Web.

2.2.10.2 OneTimePass user

The OneTimePass user shall be entitled to initiate all card/token blocking measures that globally affect all OneTimePass providers. This allows OneTimePass users to respond very quickly if a smart card or token is lost. It is therefore not necessary for the OneTimePass user to initiate blocking with every provider.

The OneTimePass user can use the OneTimePass service Web site to globally bar the card. To initiate blocking, the OneTimePass user must identify himself with his smart card number and a valid blocking password.

Blocking shall become effective immediately after the blocking password has been entered. The following blocking options are available:

- Global blocking without cancellation (in other words, blocking is final).
- Global block with repeal

A service password, which the OneTimePass user receives as follows, is necessary to activate blocking:

- Option 1

  The Deutsche Telekom Trust Center shall accept as valid blocking passwords the first five one-time passwords generated after the smart card has been activated.

- Option 2

  The OneTimePass user shall be entitled to allocate himself a service password via the OneTimePass service Web site. A valid one-time password shall be required for the activation of the blocking password.

If a OneTimePass user is not to have access to the Internet, he can instruct a provider of his choice to carry out the blocking for him.

2.2.11 System requirements

To use OneTimePass, the OneTimePass provider must meet the following system requirements:

- Internet access for administration and checks of one-time passwords
- RADIUS client that can generate/send RADIUS requests according to the RFC 2865 and RFC 2868 standard (e.g. router, web server, RAS server, etc. ...).

2.2.12 Availability

The OneTimePass service provided via the Internet is available to customers 24/7 (please refer to SLA for details).

2.2.13 Maintenance and service

These services are described in the respective OneTimePass Service Level Agreement (SLA), which can be provided to the customer upon request.

The General Supervisors listed in the OneTimePass system are informed about important changes and maintenance work via email through a newsletter function.

2.3 Features – Authentication media

Telekom Security offers different kinds of authentication media (hard- and/or software) including registered ID-number for recurrent creation of one-time passwords by the user

The different kinds of authentication media are described in the following chapters.

2.3.1 CardReader OTP-Reader III

The offline CardReader OTP Reader III with display and keyboard has the following functional range:

- One-time password generator via display and keyboard
- Support of OneTimePass
- Support of the latest card generation TeleSec NetKey 3.0 (on the basis of TCOS 3.0)

Technical data:

- Optional USB connection (via a separately available base)
- Firmware updateable (via a separately available base)

- Graphic LCD display
- Number and function keys
- removable batteries (2x CR-2025)
- Protocols T = 1 and T = 0 (ISO 7816-3).

2.3.2 NetKey 3.0 smart card

The TeleSec NetKey 3.0 smart card is an anonymized crypto smart card, i.e., it contains no personal data. The smart card is manufactured in the secure environment of the Telekom Trust Center and is used to generate the dynamic one-time password.

Basic functions:

- Intelligent processor smart card
- Delivery protection (zero PIN procedure)
- OneTimePass application
- Global card PIN (access protection)
- Global card PUK
- Failed logon attempt counter
- Evaluated smart card operating system TCOS (TeleSec Smart card Operating System)

Other useful functions:
Use of the additional features requires additional software and hardware that are not covered by this contract.

- Digital signature
- Encoding and decoding of any files
- Four certificates in accordance with ITU-T recommendation x.509v3 (see below)
- Additional personal certificates can be downloaded
- Standard applications (except OneTimePass):
  - NetKey V3.0 (three certificates)
  - SigG with keys from an E4-evaluated key generator (a certificate)
  - Physical access control
  - Time recording
  - Watermark

Technical data:

- TCOS 3.0 security operating system on the smart card
- Command structure and contents pursuant to ISO/IEC 7816-4, 7816-8
- Proprietary commands only in the case of non-standardized functions
- Asymmetrical cryptographic RSA (Rivest Shamir Adleman) procedure with a key length of 2,048 bits
- Symmetrical cryptographic methods DES (Data Encryption Standard, 56-bit), DES3 (112-bit, 168-bit), IDEA (International Data Encryption Algorithm, 128-bit) with ECB (Electronic Code Book) or CBC (Cipher Block Chaining) mode
- Secure messaging for transmission security

- Applications can be implemented in the field
- Free storage space for user-specific applications, depending on the card type
- Defense mechanisms to protect against all known attack scenarios.

When using the NetKey 3.0 in combination with OTP-Reader III, PIN and PUK are configured by the user during initialization phase (when breaking the zero-PIN).

2.3.3 OneTimePass Token III

The OneTimePass Token is a compact device that displays one-time passwords at the push of a button. The secure TeleSec smart card NetKey 3.0 is not used in this token (no migration to certificate services possible!). The tokens are personalized in the manufacturer's secure environment.

To increase security, a 4-digit server PIN is always needed for authentications that the user must enter on the service website for users (onetimepass.telesec.de). Alternatively, the OneTimePass administrator can trigger PIN generation (random number) and PIN allocation (via e-mail).

The OneTimePass Token can be used by OneTimePass users. Smart card-based solutions must continue to be used for OneTimePass administration.

2.3.4 OneTimePass SMS

With “OneTimePass SMS” the OneTimePass user receives his one-time passwords from the OneTimePass server directly via text message. The OneTimePass user uses his current cell phone and existing cell phone contract with any provider.

The one-time passwords are sent by the OneTimePass SMS gateway immediately after the mobile number has been checked for authorization . Because there is no prioritization for SMS in cell phone networks, Telekom Security cannot guarantee how long it will take from the request to the allocation of a one-time password via text message.

A new one-time password on the OneTimePass server can be requested in the following ways:

Request via text message:

Registered “OneTimePass SMS” users can request a new one-time text message password from the OneTimePass SMS gateway via their cell phones, which is subsequently allocated to them via SMS.

Request via website:

As a second alternative, registered “OneTimePass SMS” users can request a one-time password for a specified OneTimePass alias through a request that can be integrated into the respective website. The one-time password is then sent to the registered cell phone via SMS.

Pro-active sending:

Another alternative is the pro-active sending of one-time passwords via SMS. The user gets the first one-time password via SMS, when the OneTimePass Administrator has administered him in the OneTimePass platform. Each time, the user authenticates successful via RADIUS, a new password will be sent to him via SMS. The feature “pro-active sending” can be activated in the group properties from the General Supervisor.

The SMS-text can be edited from the General Supervisor for each group, to meet the needs of e.g. different user-groups for different countries.

2.3.5 OneTimePass Software token

To complete the OneTimePass portfolio, software token are provided for a variety of operating systems.

2.3.5.1 OneTimePass SoftToken for Microsoft Windows (in combination with smart card)

The TeleSec OneTimePass SoftToken is a special Windows application that takes over the generation of one-time passwords. This software is required for so-called online smart card readers (with a direct PC connection) that do not have an integrated Offline OneTimePass or SecOVID functionality (e.g., CardReader Mobile or CardReader Special). The OneTimePass SoftToken also contains all functions for efficient PIN/PUK handling.

The OneTimePass SoftToken is available in two versions for improved role allocation within your company:

With the administrator version, the OneTimePass Administrator is able to easily read out PUKs from user cards. The PUKs can be saved, printed out as a PUK letter (on regular paper or special PUK letter templates) or sent to the end-user via email. This version contains all other SoftToken functions.

The user version of the SoftToken has all the functions except for the PUK read-out functions.

Both versions are available in German and English.

The OneTimePass SoftToken can be employed on all Microsoft Windows platforms (Windows 2000, Windows XP, Windows Vista, Windows 7 32/64bit) – the installation requires about 10 MB of disk space.

A KOBIL smart card terminal is a prerequisite for operation (prerequisite: online reader, with connection to a PC) with serial, USB or PCMCIA connection, including installed ctapi or PC/SC driver.

The TeleSec OneTimePass SoftToken is included with the OneTimePass service and can be downloaded in the download area of the respective Service websites.

2.3.5.2 OneTimePass SmartToken (SMT)

To generate one-time passwords (without online connection) Telekom Security provides the OneTimePass SmartToken as pure software solution.

The application is distributed via operating manufacturer's AppStores free of charge.

After administration from the OneTimePass Administrator the user receives an activation code via email. During the first app start the software will be initialized for the usage with the OneTimePass platform. Here for an online connection via mobile network or WLAN is needed. For the usage of the SmartToken after this initialization, an online connection is not neccessary.

The user defines a PIN and a PUK. After entering a false PIN for three times, the application can only be unblocked with the PUK. After entering this PUK fort en times, the app will be locked finally and all secrets are erased to avoid misusage. For further usage of the app it has to be reinitialized.

2.3.5.2.1 SmartToken for Apple iOS

The OneTimePass SmartToken for iOS can be used in combination with an Apple iPhone, iPad and iPod Touch from iOS version 3.2 (SmartToken 1.21) or iOS version 6 (SmartToken 1.30) on.

The app is distributed free of charge via Apple AppStore:

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

2.3.5.2.2 SmartToken for Google Android

The OneTimePass SmartToken is available for smartphones and tablets with Android OS from version 5.0 and for wearables/smartwatches with Wear OS. Not running on devices with Tizen OS (Samsung Gear S2 / Gear S3 / Galaxy Watch)!

The app is distributed free of charge via Google Playstore:

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

2.3.6 Static OneTimePass users

If only the pure RADIUS functions (static/dynamic IP address allocation, etc.) are to be used, there is a possibility of creating static OneTimePass users. In addition, the static OneTimePass user can be used for automated monitoring of the OneTimePass system availability.

The static user can also be used for helpdesk purposes, if an user has lost his regular authentication media.

Approval for creating static users is only provided following an informal written request to the OTP provider.

2.3.7 System requirements

2.3.7.1 Standard Authentication Media

No special system requirements are needed for operation of the OneTimePass authentication media by the OneTimePass user because neither the OneTimePass Token nor the CardReader needs to be connected to a PC in order to use OneTimePass. No additional client software is required either. The Microsoft remote data transfer network (with network access protection) can be used as standard software on the user side, for example.

2.3.7.2 OneTimePass SMS

OneTimePass users need their current cell phone and any cell phone contract in order to use OneTimePass SMS.

Mobile network coverage is required in order to receive one-time passwords via text message. OneTimePass SMS can be used nearly worldwide with a huge number of mobile phone providers. To enroll the solution to new countries outside Europe, Telekom Security has to check the usability at first.

2.3.7.3 OneTimePass SmartToken

The requirements for the different SmartToken models can be found in the chapters 1.1.5.2.1 to 1.1.5.2.4.

2.3.8 Terms of delivery

In principle, OneTimePass authentication media are only provided to OneTimePass providers.

The OneTimePass authentication media (incl. operating manual) are distributed to OneTimePass users by the OneTimePass provider.

The TeleSec NetKey 3.0 smart card is on the dual-use list and is thus subject to the special export and import conditions that must be made transparent to the OneTimePass user.

2.4 Unilateral Service Changes

The DT Security reserves the right to make unilateral service changes and reduction in compensation in favor of the customer. The customer explicitly agrees with these adjustments. In case of deviation in the agreed written requirement, the Telekom shall inform the customer about possible changes by sending the latest versions of the existing contractual documents; these shall replace the already existing documents.

2.5 Optional Services

By agreement and subject to technical and operational feasibility, Telekom Security shall, in particular, perform the following additional Remote Connect services for an additional charge (not for the OneTimePass Compact rate model):

2.5.1 Services for Hardware (Smart Card, Card Reader and Token)

2.5.1.1 SHIPPING COSTS

International Shipping Costs:
All services will be provided within Germany. International deliveries will be separately invoiced. International deliveries will be separately invoiced.

Shipping Costs for end-users:
All services will be directly furnished to the provider. The provider will distribute the user components to the end-users. If direct delivery to the end-user is desired, this will be separately invoiced for each delivery address.

2.5.2 Validity period of one-time passwords (VPN support)

Certain applications require additional channel resources during access (e.g. VPN). In such a case, OneTimePass would activate several authentications, which would result in several entries of one-time passwords. With the channel bundling feature, the OneTimePass service provides the option of temporarily saving the one-time password for several seconds while the connection is established. This makes the required bandwidth useable when the application is authenticated.

This feature can also be used to establish an internet connection and a VPN connection with one OTP.

The validity period can be set / activated only by General Supervisor in the user group policies.

2.5.3 Provision of an interface for connection to the Trust Center

2.5.3.1 INTERFACE TO THE TRUST CENTER / MPLS

Additional to the standard connection via internet, Telekom Security offers a connection via a central MPLS-/IPLS--access. A direct connection can also be established, if the customer wishes so. If there is no MPLS access on customer’s site, the access has to be ordered by customer / OTP provider.

2.5.3.2 INTERFACE TO THE TRUST CENTER / IPSEC-VPN

Additional to the standard connection via internet, Telekom Security offers a connection via IPSEC-VPN tunneling. A direct termination can also be established, if the customer wishes so.

2.5.3.3 INTERFACE TO THE TRUST CENTER / INDIVIDUAL

If the customer so desires, an individual connection between the OneTimePass provider and the Telekom Trust Center can be established. This service is separately estimated and invoiced.

2.5.4 Administration workshop

Telekom Security holds a one-day OneTimePass workshop (5 hours) on its premises. The workshop is serves for administration of OneTimePass in all hierarchies (General Supervisor,

Supervisor, Administrator, User). During this workshop, all available functionalities of the service websites are shown.

2.5.5 Customized Layout of the Service Website

A customized layout of the service website is generally separately estimated and invoiced at a fixed price. The technical framework of the website is provided.

Telekom Security will give the provider a document listing the changes that are possible.

2.5.6 Customized Language

The OneTimePass website is provided in German, English, French and Dutch. Implementation of another language is only possible in conjunction with a customized layout of the website and is additionally invoiced at a fixed price. Telekom Security will give the provider an MS Excel document with the texts as the source language for the new translation.

2.5.7 OneTimePass Consulting

Complex services and individual requirements will be separately estimated and invoiced per requirement.

3 Customer’s obligations to cooperate

The OneTimePass customer maintains the connection of his active network components (router) to the T-Systems Trust Center. For the connection the standard RADIUS (Remote Autnetication Dial-In User Service (rfc2865 / rfc2868)) is requested. The customer ensures, that his active network components support the RADIUS protocol.

The OneTimePass customer (OneTimePass Provider) provides staff to administrate and manage his OneTimePass-users.

Therefore the following management groups / hierarchies are required:

<u>OneTimePass Compact</u>
OneTimePass Administrator

<u>OneTimePass Advanced</u>
OneTimePass General Supervisor
OneTimePass Supervisor
OneTimePass Administrator

4 Minimum provision period/termination

The minimum duration of a TeleSec OneTimePass contract is 12 months. It can be terminated 3 months prior to the contract termination in written form.
The contract will be extended automatically by 6 months, if not being cancelled on the due date.

Additional documents

General Terms and Conditions (GTC)

The General Terms and Conditions of TeleSec OneTimePass of Telekom Security International GmbH that are valid at the time of contract signing are applicable.

Service Level Agreement (SLA)

The respective Service Level Agreement (SLA) contains information about the availability, maintenance and service.

List of abbreviations / Glossary

Abbreviation	Description
E4 "high"	Evaluation levels according to ITSEC - E4 = evaluation level , "high" = mechanism strength
ITSEC	Information Technology Security Evaluation Criteria.
RA	Registration authority for registering and identifying users for certain services.
RADIUS	**R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice – a standard for authenticating and accounting for remote access dial-in users. RADIUS allows communication between a dial-in server and an authentication server.
RFC	**R**equest **F**or **C**omments – the Internet Engineering Task Force (IETF) comprises numerous task groups whose working results are published as RFCs. Depending on their form, RFC documents may be treated as a standard. Examples: RFC 2138 – describes the authentication RFC 2139 – describes the accounting
SSL	**S**ecure **S**ocket **L**ayer – protocol for secure online data transmission between clients and servers on the Internet. Sensitive data is transferred over the World Wide Web in an encrypted format and so that it cannot be intercepted. This protocol (X.509 standard) was developed by Netscape and is supported by all common browsers.
TCOS	TeleSec Chipcard Operating System – Smart card operating system that was developed by TeleSec and is today the most secure system in the world.
TTC	Telekom Trust Center