Service Specifications & Additional Terms and Conditions Magenta Security OneTimePass.ID

Last revision: 01.07.2022

<This document is a convenience translation of the German original. In case of discrepancy between the English and German versions, the German version shall prevail.>

Publication details

Published by

Deutsche Telekom Security GmbH

Bonner Talweg 100

53113 Bonn

Germany

hereinafter referred to as “Telekom”

WEEE reg. no. DE 56768674

CONTENTS

1 INTRODUCTION

Magenta Security OneTimePass ID – hereinafter referred to as OneTimePass – offers strong 2-factor authentication based on a dynamic one-time password system.

The service uses various tokens (authentication media) to generate one-time passwords for logging in to online services and protected systems of the customer (OneTimePass provider). Separate user administration is available via online service portals for the administration and assignment of the authentication media to the customer's users.

Administration is tiered into a total of four authorization levels (general supervisor, supervisor, administrator, and user) to be able to adapt these flexibly to customer requirements and customer structures (branches, departments, etc.).

The OneTimePass service is operated in the highly secure and certified Telekom Trust Center.

The provider of the Trust Center services and products is Deutsche Telekom Security GmbH, hereinafter referred to as Telekom.

2 FUNCTIONS – AUTHENTICATION MEDIA

Telekom sells the customer (hereinafter: OTP Provider) OneTimePass authentication media (hardware and/or software) for the recurring generation of one-time passwords by the user. The various authentication media are described in the following sections:

2.1 Card reader – OTP Reader III

The offline card reader OTP Reader III with display and keyboard is used to generate one-time passwords for OneTimePass. Smartcards up to TCOS 3.0 are supported. The batteries (button cells 2x CR-2025) can be easily replaced.

2.2 NetKey 3.0 chip card

The NetKey 3.0 TCOS chip card is an anonymized crypto chip card, i.e., it does not contain any personal data. The chip card is manufactured in the secure environment of the Telekom Trust Center and is used to generate the dynamic one-time password.

If the NetKey 3.0 is used with the OTP Reader III, both the PIN and the PUK are defined by the user when the card is initialized (breaking the null PIN).

2.3 OneTimePass Token III

The OneTimePass Token is a compact device that displays one-time passwords at the touch of a button. No chip card is used in these tokens (migration to certificate services is not possible!). The tokens are personalized in a secure environment of the manufacturer. The transmission of secrets from the manufacturer to Telekom is always encrypted.

To increase security, authentications always require a 4-digit server PIN that users must define for themselves on the service website for users (onetimepass.telesec.de). Alternatively, PIN generation (random number) and PIN distribution (by email) can be triggered by the OneTimePass administrator.

The OneTimePass Token can be used by OneTimePass users. Using the OneTimePass Token for OneTimePass administration is also possible once it has been approved by of the provider.

2.4 OneTimePass SMS

With “OneTimePass SMS,” the OneTimePass user’s passwords are sent directly to them by text message (SMS). OneTimePass users use their current cell phone and their existing cell phone contract with any cell phone provider. OneTimePass SMS can be used almost anywhere in the world. Telekom is not responsible for ensuring that text messages (SMS) are received. This is the responsibility of the customer in conjunction with the mobile communications provider on the user side.

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

For instructions on how to use the SMS token, please refer to the associated user manual.

2.5 OneTimePass software token

To complete the portfolio, software tokens are offered for various operating systems (further tokens for mobile devices are currently in preparation).

2.5.1 OneTimePass SoftToken for Microsoft Windows (in connection with Smartcard)

The OneTimePass SoftToken is a special Windows application that handles the generation of one-time passwords. The OneTimePass SoftToken uses an existing chip card in an installed card reader to generate one-time passwords.

This software is required for online chip card readers (with direct connection to a computer) (e.g., an existing card reader at the workplace or integrated card reader in a notebook). In addition, the OneTimePass SoftToken includes all functions for efficient PIN/PUK handling.

The OneTimePass SoftToken is included in the scope of delivery of the OneTimePass service and can be downloaded from the download area of the respective service web pages.

The OneTimePass SoftToken is available in two languages: German and English.

A Microsoft Windows platform (Windows 10/11) is required to use the OneTimePass SoftToken.

This requires any kind of chip card terminal (prerequisite: online reader, meaning it is connected to a PC) that can be used under Windows.

2.5.2 OneTimePass SmartToken (SMT)

Telekom offers the OneTimePass SmartToken as a pure software solution for generating one-time passwords.

The application is available via the app stores of the operating system manufacturers.

After the solution has been set up by the OneTimePass administrator, users are sent an email with an activation code. When the app is started for the first time, the parameters are set/initialized for use with the OneTimePass platform. An online connection is required for this. No internet connection is required to use the SmartToken following successful initialization.

The user defines a PIN and a PUK to use the SmartToken. For further instructions on how to use the SmartToken, please refer to the associated user manual.

2.5.3 SmartToken for Apple iOS

The OneTimePass SmartToken for iOS can be used in conjunction with an Apple iPhone and iPad from iOS version 11.0 or higher (SmartToken 1.21), as well as in conjunction with the Apple Watch.

The app is distributed via the Apple AppStore:

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

2.5.4 SmartToken for Google Android

The OneTimePass SmartToken is available for smartphones and tablets with Android operating system version 5.0 or higher, as well as for wearables/smartwatches with Wear OS.

The app is distributed via the Google Play store:

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

2.6 Static OneTimePass users

A static OneTimePass user can be used for automated monitoring of OneTimePass system availability.

Static users are also useful for a service desk to temporarily and at short notice restore users who have lost their authentication media so they can continue working. The approval for creating static users is given by the OTP provider only after submission of an informal written order.

2.7 System requirements

2.7.1 Standard authentication media

In principle, no special system requirements are necessary for the OneTimePass user to operate the OneTimePass authentication media. No additional client software is required.

2.7.2 OneTimePass SMS

To use OneTimePass SMS the OneTimePass user needs a current cell phone and any kind of cell phone contract.

Mobile network coverage is required to receive the one-time passwords via text message (SMS). OneTimePass can be used almost anywhere in the world with many mobile service providers. Unrestricted SMS reception depends on the respective network operators and national regulations and cannot be guaranteed.

2.7.3 OneTimePass SmartToken

For the requirements for using the SmartToken, please refer to Section 2.5.

3 SERVICES PROVIDED BY TELEKOM

3.1 Initial provision – Rate models

Various rate models are available to the customer with the OneTimePass service.

3.1.1 OneTimePass price model

OneTimePass users are charged a flat monthly fee (depending on the user tier used) and are independent of the number of authentications. The initial provision of the service includes the delivery of two OTP Readers III and two SmartCard NetKeys 3.0 for administrators. This model is suitable for any number of users. The following scales or packages are available under the OneTimePass rate model:

OneTimePass 10, ... License

With the OneTimePass (10, 25, 50, 100, 250, 500, 1,000, 2,500, 5,000, 7,500, 10,000, and 10,000+) License, the service is provided to the customer for a limited number of users depending on the package chosen. This is irrespective of the number of OneTimePass user groups in which the OneTimePass user is administered. The price scales can be changed by upgrading or downgrading.

OneTimePass Extension 25, ...

The OneTimePass Extension (25, 50, 100, 500, and 1,000) allows the customer to change the number of users in smaller increments. This means that the OneTimePass 1,000 (= 1,000 users), for example, can be extended by a OneTimePass Extension 500 (= 500 users) to increase the number of users to a total of 1,500. The OneTimePass Extension packages remain in the service portfolio until they are canceled and are not offset against a OneTimePass upgrade or downgrade.

If, for example, the customer upgrades from a OneTimePass 1,000 to a OneTimePass 2,500, the Extension 500 continues to apply unless it has been canceled. The total number of users available to the customer is therefore 3,000.

The Extension volume cannot be larger than the volume of the ordered OneTimePass package. This means that Extensions 500 and 1,000 cannot be used with the OneTimePass 100 or 250.

3.1.2 OneTimePass trial period

The trial period is a service that is unrestricted in terms of scope of services, and there are no monthly costs. Only a one-time provisioning fee is charged for the trial period and includes two OTP Reader III, two SmartCard NetKey 3.0, and five OneTimePass Token III. The maximum term of a trial period is 3 months (or by agreement). If an order is placed after the trial period, the initial provision charge will be offset against the order.

3.1.3 OneTimePass reseller

If you are interested in reselling OneTimePass, please get in touch with your Telekom contact person.

3.1.4 Terms of delivery

OneTimePass authentication media is generally delivered to OneTimePass providers only (exceptions at additional cost),

who will then distribute the OneTimePass authentication media (incl. user guide) to the OneTimePass users.

The NetKey 3.0 TCOS chip card is listed in the dual-use list and is therefore subject to special export and import regulations (restrictions on use abroad may have to be observed).

3.2 Operation

The central authentication service is operated by Telekom in the Telekom Trust Center and given to the provider for the agreed contract term.

The server protected by OneTimePass sends an electronic validity request (Standard **R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice (RADIUS) in accordance with protocol RFC 2865 and RFC 2868) to the OneTimePass platform in the Telekom Trust Center over the internet. This server checks the validity of the one-time password and returns the attributes set for the corresponding user or group profile. Alternatively, the connection can also be established via SOAP or federation services.

The Telekom Trust Center will not associate the request with an actual person; only the card identification number and/or the alias name will be known.

3.2.1 OneTimePass service platform

Telekom operates a central OneTimePass services platform in the Telekom Trust Center, which checks the submitted one-time passwords of the OneTimePass provider for validity. All providers are administered in the services platform. Each provider can in turn administer individual groups and profiles. This central administration allows the OneTimePass authentication media (see Item 2) to be used for different applications with different providers, but only if they have been activated by the respective provider.

3.2.2 OneTimePass group

The OneTimePass provider is given the opportunity to divide users into “user groups” in order to distinguish or identify them according to applications and customer groups/departments (Controlling, Sales, etc.). All users in a group can be assigned the same RADIUS attributes if desired. This simplifies the administration of individual users. The OneTimePass provider has the option to define a limit for the number of OneTimePass users in the OneTimePass group. The number of OneTimePass groups can be limited by Telekom depending on the price model or proposed package.

3.2.3 OneTimePass administration on the customer’s side

For the administration of the OneTimePass service, each provider is given 2 of the maximum 10 possible general supervisor authorizations with the OneTimePass authentication medium “SmartCard with OTP Reader III” for identification on the Trust Center’s internet service pages.

All other functions and authorizations of the total four-level service portals (general supervisor, supervisor, administrator, user) are administered by the provider and described in the relevant manuals.

3.2.4 OneTimePass user

OneTimePass users are identified by the OneTimePass provider and receive an authentication medium assigned to them. User administration is carried out via the Trust Center’s service web pages. The authorizations or services are described in the relevant user manual.

3.2.5 One-time password check

OneTimePass is what is known as two-factor authentication based on the two factors “possession” and “knowledge.” Depending on the type of authentication medium used, a 4-digit server PIN is required.

Therefore, when a user makes an authentication request, the alias name of the user and their one-time password (8 digits), and, if necessary, the server PIN (4 digits) are transmitted.

The OneTimePass system knows the next 15 passwords. If this framework is exceeded (e.g., generation of passwords without using them for authentication purposes), there is the option of synchronization.

3.2.5.1 RADIUS

In order to use the OneTimePass Standard service, the provider usually only needs its existing infrastructure (such as a router, VPN gateway, or similar) and the RADIUS protocol (RFC 2865 and RFC 2868) to connect to the Trust Center. The OneTimePass service only includes the authentication of the user.

3.2.5.1.1 RADIUS – user profile

Telekom provides the OneTimePass provider with the RADIUS attributes in accordance with RFC 2865 and RFC 2886. These attributes can be assigned to a OneTimePass group or a

OneTimePass user. Administration is carried out via the service web pages of the Telekom Trust Center.

3.2.5.1.2 RADIUS – rules

The OneTimePass platform supports the creation of sets of rules that make it possible to define for a particular group which actions (output attributes) are carried out under what conditions (input attributes). Collectively, the conditions and actions are referred to as events. The rules are administered via the service web pages for administrators.

3.2.5.2 Federation services

Federation services were added to the existing interfaces, enabling customers to perform OneTimePass authentications via SAML 2.0 and OpenID Connect.

This interface enables users to implement a SingleSignOn between multiple SAML service providers or OpenID Connect clients at OTP group level.

The federation services are only used for authentication; extended authorization functionalities are not supported in the current configuration.

The settings required to use the federation services are made via the General Supervisor Service web pages.

The federation services include the following:

- SAML 2.0
- OpenID Connect
- REST API

If you are interested in the federation services, a detailed documentation can be provided upon request. For further instructions on how to use the federation services, please refer to the associated user manual.

3.2.6 OneTimePass administration

3.2.6.1 Internet service portal – providers

Telekom provides four service portals to the customer. The core functions include:

OneTimePass general supervisor

The general supervisor is the highest authority for administering the OneTimePass service. The smartcards supplied (or additionally ordered if required) together with the OTP Reader III are provided for use. A maximum of 10 general supervisors can be set up. This authorization is used to set up the basic functionalities and features, as well as to set up user groups and the associated supervisors.

OneTimePass supervisor

Supervisors can have authorization for one or more user groups (depending on the configuration of the general supervisor) and manage the administrators of their user groups for this purpose.

OneTimePass administrator

Administrators can be authorized for one or more user groups (depending on the configuration of the supervisor) and manage the assignment of users to the authentication media used in their portal.

OneTimePass user

For the user, there is a portal for self-administration (FAQ, download of manuals, PIN management, barring in case of loss).

All other functions are described in detail in the respective user manuals, which are available in the download area of the particular hierarchy or from Telekom on request.

3.2.6.2 SOAP administration

An alternative to using the service web pages for OneTimePass administration is SOAP-based administration. The administrative tasks have been replicated in the form of specified SOAP calls and are provided as an Application Programming Interface (**API**). This means that an existing administration portal can easily be connected to OneTimePass. Authentication is performed using a client certificate of the Server.ID. The "OneTimePass SOAP-Spezifikation Vn.pdf" document, which can be obtained optionally, contains the full command set, including WSDL description.

3.2.6.3 Bulk administration

The bulk administration (in the service portal for administrators or via SOAP) offers the functions for bulk administration, snapshots, and user exports for efficient simultaneous management/administration of many users.

Bulk administration allows the creation, modification, or deletion of up to 5,000 data records. Data records are transferred in CSV format, using a semicolon as a delimiter.

Two more powerful tools are available with the snapshots (backup before bulk import) and user export functions. Detailed instructions can be found in the user manual for administrators.

3.2.6.4 Internet service portal – users

Telekom operates a self-administration portal for OneTimePass users with the following functions:

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

3.2.7 Barring service

Since OneTimePass is a centralized service, the OneTimePass users can use the OneTimePass authentication medium to log into several OneTimePass providers without negatively affecting their application or compromising their secure access. For this reason, OneTimePass distinguishes between different barring options for users and administrators.

For further information on barring options, please refer to the corresponding manuals.

3.2.8 System requirements

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

3.2.8.1 RADIUS

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

3.2.8.2 SOAP

- Internet access for administration and checks of one-time passwords where necessary
- SOAP client that can present a valid client certificate for using the API functions provided (customer's own contribution).

3.2.8.3 Federation services

- Internet access for administration as general supervisor, for federation services activation, and for configuration of the necessary parameters.

3.2.9 Availability

The OneTimePass service provided online can be accessed by customers 24/7. More accurate details on availability and service levels can be found in the service level agreement (SLA), as amended.

3.2.10 Maintenance and service

This service is described in the applicable OneTimePass service level agreement (SLA), which can be provided to the customer upon request.

A newsletter functionality can be used to inform the general supervisors listed in the OneTimePass system about important changes or maintenance work by email.

3.3 Optional services

Where technically and operationally feasible, Telekom will provide the following additional services subject to agreement and a separate fee):

3.3.1 Services – hardware

3.3.1.1 Shipping costs

International shipping costs:

All services are rendered in Germany. Deliveries to other countries will be billed separately.

Shipping costs for end users:

All services are delivered directly to the provider. The user components are distributed to the end users by the provider. If direct delivery to the end user is requested, this will be billed separately for each delivery address.

3.3.2 Period of validity of the one-time passwords (VPN login)

To use the one-time passwords for two successive authentications (e.g., for VPN to establish the internet connection followed by the authentication of the VPN tunnel), the general supervisor has the option to explicitly extend the validity period for a user group by a few seconds.

3.3.3 Interface for connection to the Telekom Trust Center

The standard connection to the Trust Center is an unencrypted internet connection. Special connections are additionally offered as an option.

3.3.3.1 Interface to the Trust Center/MPLS

In addition to the standard connection over the internet, Telekom offers a connection to the Trust Center via a central MPLS/IPLS connection. A direct connection can be set up if requested by the customer. If no MPLS connection is available on the customer's side, the customer is personally responsible for applying for the connection.

3.3.3.2 Interface to the Trust Center/IPSEC VPN

In addition to the standard connection via the internet, Telekom offers a connection to the Trust Center via an IPSEC/VPN tunnel. A direct termination can be set up if requested by the customer.

3.3.3.3 Interface to the Trust Center/individual

If requested by the customer, an individual connection between the OneTimePass provider and the Telekom Trust Center can be established. This service is implemented and billed in a separate project.

3.3.3.4 Protocols

3.3.3.4.1 RADIUS

Authentication requests are usually sent via the established, high-performance RADIUS protocol (RFC 2865/2868).

3.3.3.4.2 SOAP

All administrative processes carried out via the service web pages can also be transferred automatically via the SOAP protocol. The Telekom Trust Center provides relevant certificates for this purpose. Authentications can be transferred via SOAP (due to its low performance, this interface is not suitable for high volume requests).

3.3.3.4.3 Federation interface

The connection can be set up via SAML 2.0, OpenID Connect, or REST API.

3.3.4 Administration workshop

Telekom conducts a one-day OneTimePass workshop at the customer's premises. The purpose of this workshop is to train OneTimePass general supervisors, supervisors, and administrators. The service portals and the available functions will be explained as part of the workshop using practical examples.

3.3.5 Customized layout of the service website

A customized layout of the service website is generally subject to a separate project and a fixed price is charged for it. The technical framework of the website is specified by Telekom.

Telekom furnishes the provider with a document that shows which changes are possible.

3.3.6 Customized language

The OneTimePass website is provided in German, English, and French. It is only possible to implement other languages if a customized layout of the website has been chosen, and an additional fixed price is charged for this. Telekom furnishes the provider with an MS Excel document containing the existing texts of the available languages as the source language for the new translation.

3.3.7 OneTimePass consulting

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

4 THE CUSTOMER'S DUTIES TO COOPERATE

The OneTimePass customer will support the connection of his active component (router) to the Telekom Trust Center. The RADIUS (**R**emote **A**uthentication **Di**al In **Us**er (RFC 2865 and RFC 2868)) standard protocol is used for the connection. Alternatively, a connection can also be made via SOAP or federation services.

The customer will ensure that the active components support the respective valid protocol.

The OneTimePass customer (OneTimePass provider) will appoint employees for the set-up and independent administration of the users of the OneTimePass service.

The following administration groups/hierarchies are required for this:

- OneTimePass general supervisor
- OneTimePass supervisor
- OneTimePass administrator

5 MINIMUM TERM/TERMINATION

The minimum lease period for OneTimePass is twelve months from the date the agreement is signed and is automatically extended by six months unless terminated with one month's notice to the end of the minimum lease period or the respective extension period.

6 OTHER APPLICABLE DOCUMENTS

The following documents apply in addition to these Service Specifications:

- GTC DTSec IT Services
- GTC DTSec Purchase and Lease of Hardware

7 GLOSSARY/ABBREVIATIONS

Term	Description
E4 "high"	Evaluation levels according to ITSEC - E4 = evaluation level, "high" = mechanism strength
ITSEC	Information Technology Security Evaluation Criteria: German: criteria for the evaluation of security in information technology.
RA	Registration authority = office to register and identify users of particular services.
RADIUS	Remote Authentication Dial In User Service – a standard for authenticating and accounting for remote access dial-in users. RADIUS enables communication between a dial-in server and an authentication server.
RFC	Request For Comments – The Internet Engineering Task Force (IETF) comprises numerous working groups, the results of whose work are published as RFCs. Depending on their form, RFC documents may be treated as a standard. Examples: RFC 2138 – describes the authentication/authorization process RFC 2139 – describes the accounting process
SigG	German Digital Signature Act (*Signaturgesetz*)
TLS	Transport Layer Security – protocol for secure online data transmission on the internet between client and server. 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) is supported by all common browsers.
TCOS	TeleSec Chipcard Operating System – chip card operating system that was developed by TeleSec and is one of the most secure in the world today.
TTC	Telekom Trust Center