


# SMARTTOKEN USER GUIDE

Magenta Security OneTimePass.ID

Deutsche Telekom Security GmbH

Version 1.3 EN
Last revised 01.04.2023

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

Management Board: Thomas Tschersich (spokesman), Dr. Klaus Schmitz

Trade Register: District Court Bonn HRB 15241,
Registered Office Bonn |
Tax ID No. DE 254595345 |
WEEE-Reg.-No. DE 56768674

| | |
|---|---|
| Brief description: | This document is the user guide for the Magenta Security OneTimePass.ID SmartToken. |
| Filename: | OTP_Userguide_SmartToken_1.3_EN_Bastelversion.docx |
| Document number: | n.n. |
| Document name: | OneTimePass SmartToken user guide |
| Version: | 1.3 EN |
| Date: | 01.04.2023 |
| Status: | Released |
| Classification: | Public |
| Last revised: | 04.04.2023 |
| Author: | Telekom Security, Ralf Kosczor |
| Content checked: | Telekom Security, Klaus Jungbluth |
| Released by: | Telekom Security |
| Contact: | TeleSec_Support@telekom.de |

© 2023 All rights reserved, including those of partial reproduction, electronic or photomechanical reproduction and evaluation by data processing methods.

# Revision history

| Version | Date | Party responsible | Changes/comments |
|---|---|---|---|
| 1.0 | 15.12.2014 | T-Systems | |
| 1.1 | 13.01.2017 | T-Systems | Alternations to layout, update |
| 1.2 | 18.11.2019 | T-Systems | Adjustment available versions, change in organization |
| 1.3 | 01.04.2023 | DT-Security | Adjustment to layout, new product name |

# CONTENTS

**1 INTRODUCTION** ..... 5
**2 DOWNLOAD AND INSTALLATION** ..... 6
**3 ADMINISTRATION OF ONETIMEPASS.ID** ..... 7
**4 ACTIVATION** ..... 8
**5 USING THE SMARTTOKEN** ..... 11
5.1 Generating one-time passwords ..... 11
5.2 Using the +Code procedure ..... 13
**6 CHANGING PIN OR PUK** ..... 18
**7 FORGOTTEN PIN OR PUK** ..... 20
**8 RE-INITIALIZATION** ..... 22
**9 CONTACT FOR FURTHER QUESTIONS** ..... 25
**10 LIST OF FIGURES** ..... 26

# 1 INTRODUCTION

Thank you for choosing Magenta Security OneTimePass.ID SmartToken from Deutsche Telekom Security GmbH (hereinafter referred to as Telekom Security).

The OneTimePass.ID SmartToken is a further authentication medium for generating one-time passwords for the Telekom Security service “Magenta Security OneTimePass.ID” (for more information see http://www.telesec.de ).

The SmartToken is a software token, meaning the creation of one-time passwords is performed by the software and you do not need any specific hardware, such as a SmartCard or similar equipment.

The SmartToken works on all smart phones and / or tablets with

- Google Android OS from version 7.0
- Apple iOS-operating system from version 11.0 and watchOS from version 3.1

⚠ For initial activation of the token or a re-initialization, you also require an internet connection via wireless LAN or the mobile communications network. This will be only required for subsequent use if versions of the Smart-Token or of the operating system of the smart phone or tablet will change.




Figure 1: Initial screen

# 2 DOWNLOAD AND INSTALLATION

To download the OneTimePass.ID SmartToken app to your terminal device, you need to log in to the respective AppStore. You will find the app there under the following links:

Android: https://play.google.com/store/search?q=telesec%20onetimepass&hl=en

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

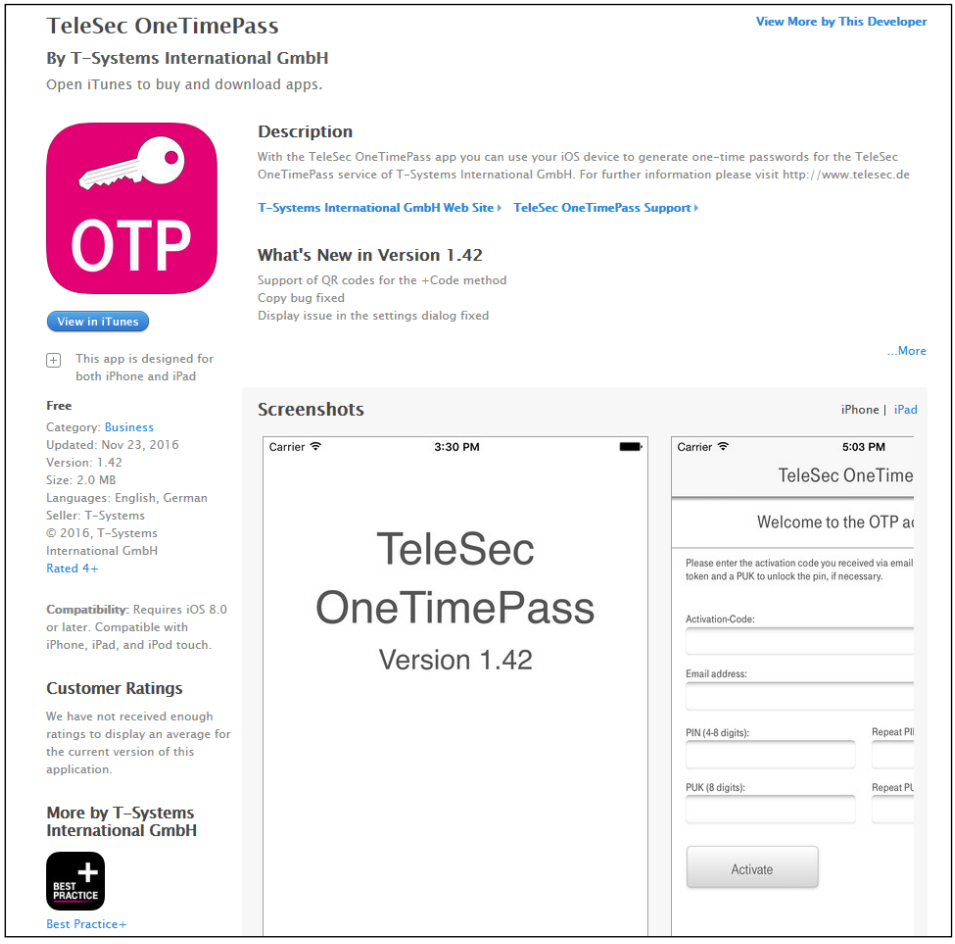



Figure 2: Smart-Token app on Apple iTunes Store

It is best to download the app directly to your terminal device, but it is also possible to download it to a PC to transfer it to the device via synchronization afterwards. The app automatically recognizes the system language and starts in either German or English.

# 3 ADMINISTRATION OF ONETIMEPASS.ID

To use the OneTimePass.ID SmartToken app as an authentication medium together with the OneTimePass.ID service, the OneTimePass.ID Administrator (within your organization) responsible for your organization first needs to set you up in the system.

After successful administration, you will receive an automatic activation e-mail to the e-mail address you have provided. This e-mail will contain the activation code for your Smart-Token from the sender noReply@onetimepass.de.

Sehr geehrte Kundin, sehr geehrter Kunde, Ihr OneTimePass-SmartToken wurde soeben durch Ihren Administrator angelegt.

Mit dem folgenden Aktivierungs-Code können sie die Initialisierung abschließen:

Aktivierungs-Code: abcd1234
Benutzername : xyz321

Bitte verwenden Sie Ihren SmartToken wie im Handbuch beschrieben.

Um OneTimePass in vollem Umfang nutzen zu können, ist die Definition eines Servicepasswortes erforderlich.
Hierzu melden Sie sich bitte als User mit Ihrer Tokennummer und einem gültigen OneTimePasswort an der Benutzeroberfläche der OneTimePass Internetseite an (https://onetimepass.telesec.de).
Wählen Sie im Menü den Punkt "Servicepasswort". Hier können Sie ein individuelles Servicepasswort festlegen.

-
- Bitte antworten Sie nicht auf diese EMail. Sollten Sie Fragen haben oder
- Informationen benötigen, wenden Sie sich bitte an Ihren Provider.
-

---

Dear customer,

Your OneTimePass SmartToken has been created by your administration service.

Please follow your User Guide to complete the initialisation procedure.
You will need to use the following activation code during the initialisation procedure:

activation code : abcd1234
user name : xyz321

If you are unsure how to use the SmartToken please refer to the User Guide for further details.
For additional information or any questions please contact your service desk.

To use OneTimePass in its entirety the definition of a service password is needed.
For this please log on as user to the service web sites (https://onetimepass.telesec.de) with your toke number and a valid one time password.
Choose the menu point "service password". There you can set an individual service password.

Please do not reply to this message.

Figure 3: Activation email

# 4 ACTIVATION

The first time the app is started, the following activation screen appears:

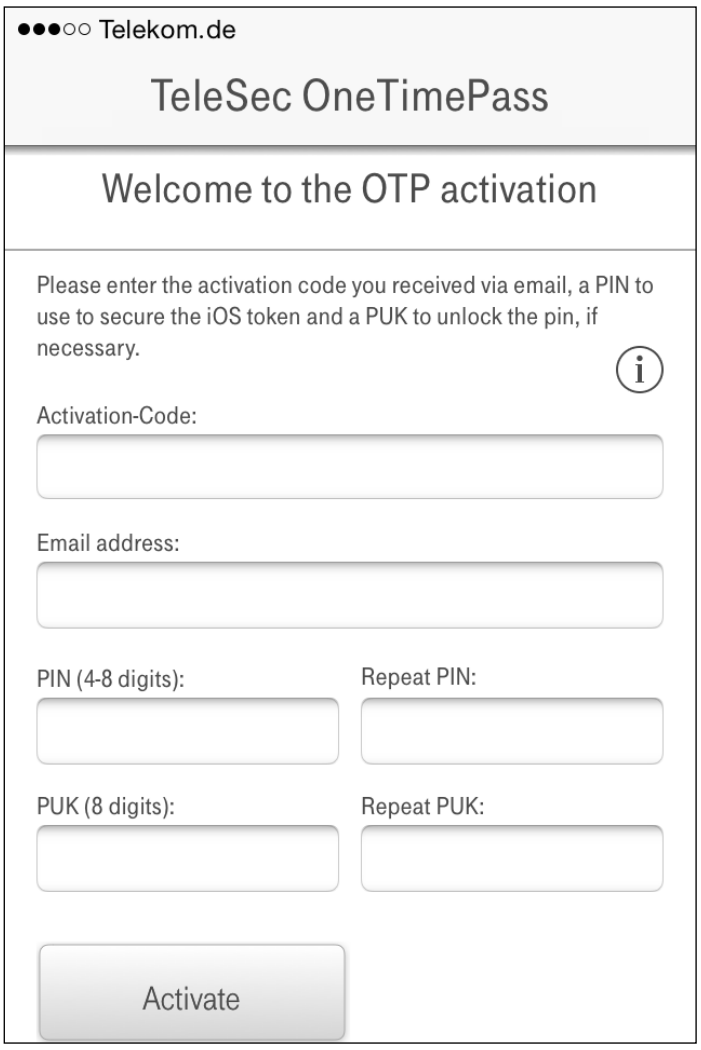



Figure 4: Activation screen

In addition to the activation code (sent by email) and the email address, where the activation code was sent to, you need to assign a PIN (personal identification number) and PUK (PIN unblocking key) here. The PIN is used to secure the application and must be entered every time you use it; the PIN must have a length of between 4 and 8 digits. Both PIN and PUK are not stored on your terminal device and not on the OneTimePass.ID platform! Secrets will be generated from PIN and PUK and these secrets will be stored on the device.
If you accidently enter an incorrect PIN three times in a row, you can unblock the application using the PUK. The PUK must have a length of 8 digits and permanently blocks the application if you enter it incorrectly ten times in a row. The Smart-Token then becomes unusable and needs to be reactivated.

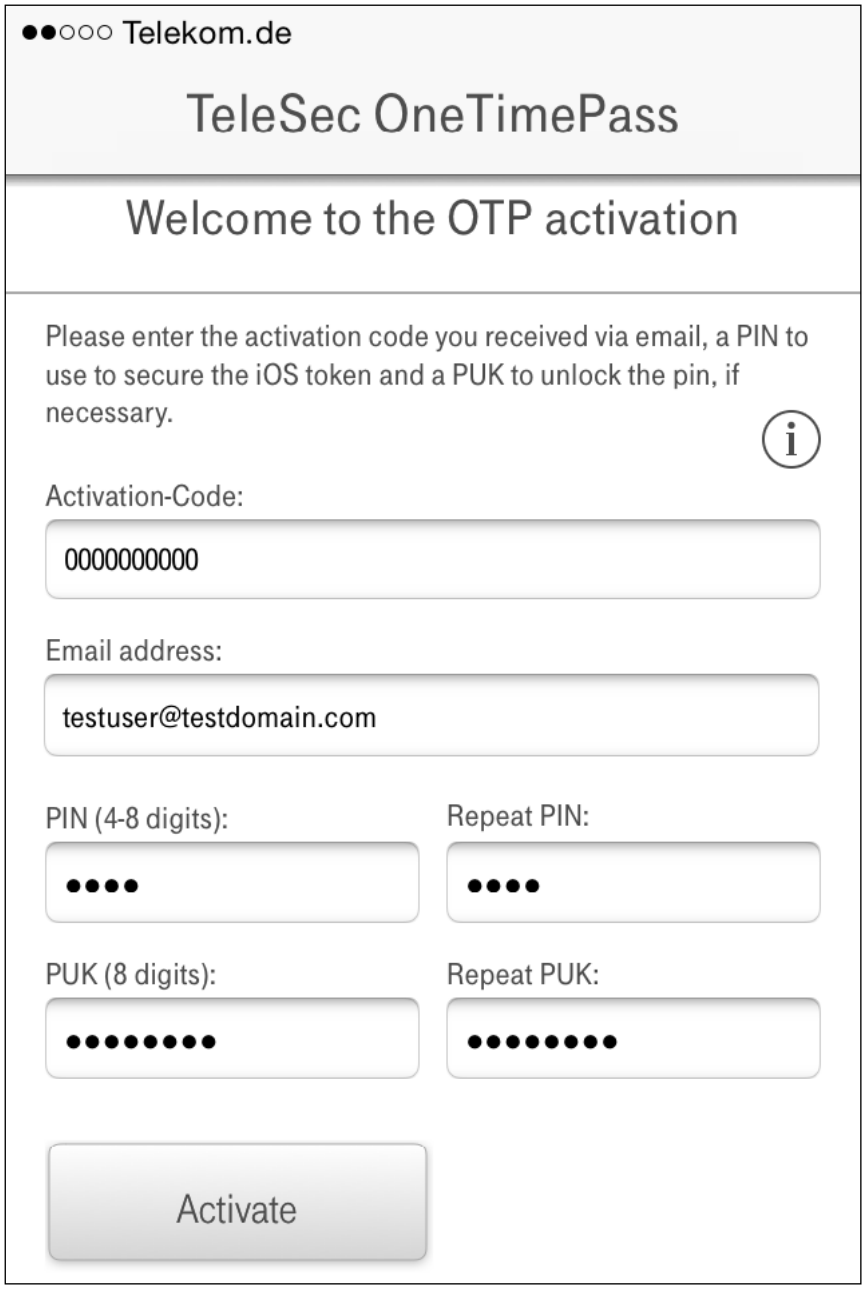



Figure 5 Entering PIN and PUK

⚠ Do not write /save the PIN and PUK on the device, otherwise anyone who gets hold of your device will be able to generate a one-time password under your name!

⚠ You have to use the same email address as used for the activation email (if necessary the email address can be changed by the administrator). Within activation no blanks may be prefixed or attached to the activation code.

Fill out the required fields and confirm your entries by touching the “Activate” button.

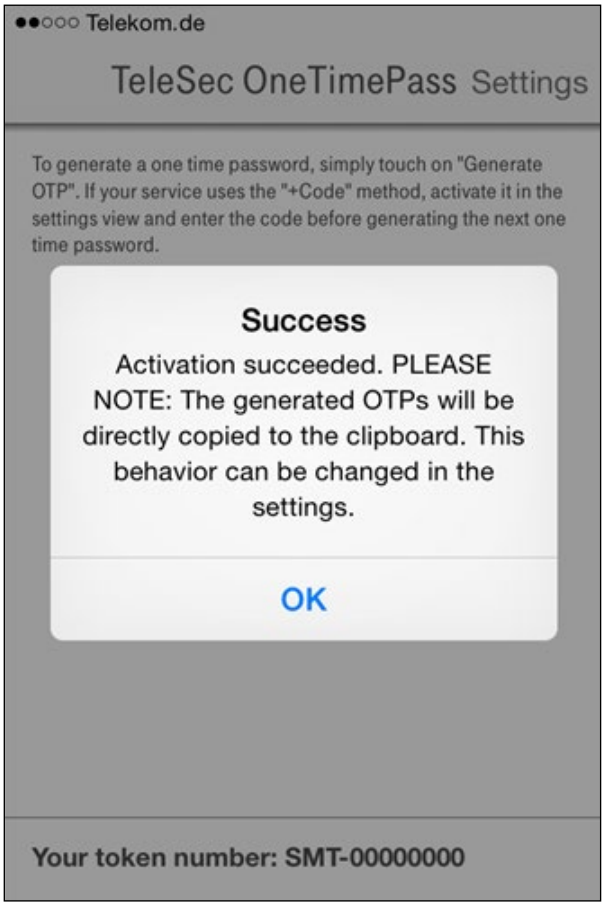



Figure 6: Successful activation

⚠ During the activation process, you require an Internet connection via wireless LAN or your mobile network provider.

As soon as the activation process has been completed successfully, you will receive a corresponding success notification.

⚠ You should remember or make a note of the token number assigned by the system as you will need this, if your Smart-Token needs to be reinitialized.

The most common source of error during the activation of the SmartToken are typing errors or accidently adding a blank to the activation code or email address. If there is a large number of activation requests within a short period of time, further requests will be rejected for a certain period of time. This serves to protect your SmartToken of unauthorised activation.

# 5 USING THE SMARTTOKEN

## 5.1 Generating one-time passwords

After you have successfully activated your Smart-Token, the main view is displayed. This is where you can generate one-time passwords.
For security reasons, every time the app is started, the PIN must be reentered in order to generate one-time passwords.

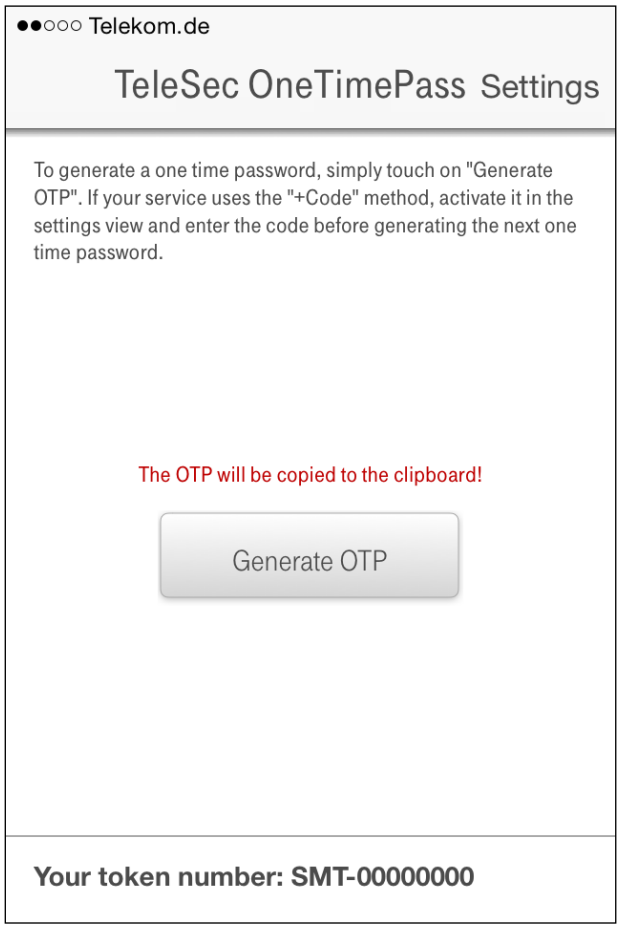



Figure 7: Start screen of the ready-to-use SmartToken

This view also shows the token number assigned by the system, which you need, for example, if you wish to log on to the user service website. Here, you can synchronize and block your token. You can reach us using this URL: https://onetimepass.telesec.de/.

To create a password, simply touch the “Generate OTP” button. The one-time password that is generated then is displayed in the form of a dialog.

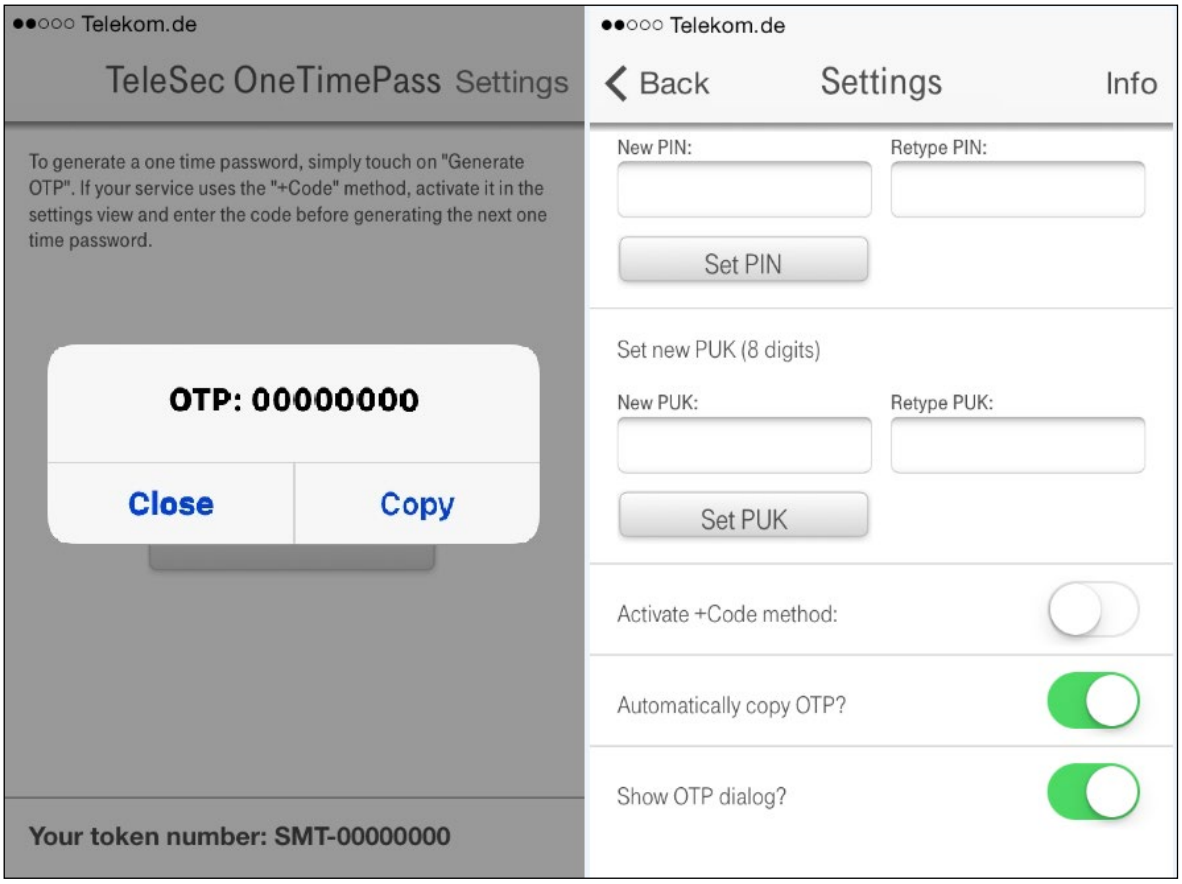



Figure 8: Generated one-time password in the OTP-Dialog & OTP-Settings

To use the one-time password directly on the device, the dialog provides the option of copying it to the clipboard and pasting it into a text field in any application. To do this, press “Copy”.
If you do not need the OTP on the device, you can close the dialog using “Close”.

## 5.2 Using the +Code procedure

The Smart-Token can also be used for the challenge-response procedure called “+Code”.

If the service that you wish to use with your Smart-Token uses the “+Code” procedure, you first need to activate this in the settings. To do so, open the Settings menu using the “Settings” button and activate the button for the “+Code” procedure.

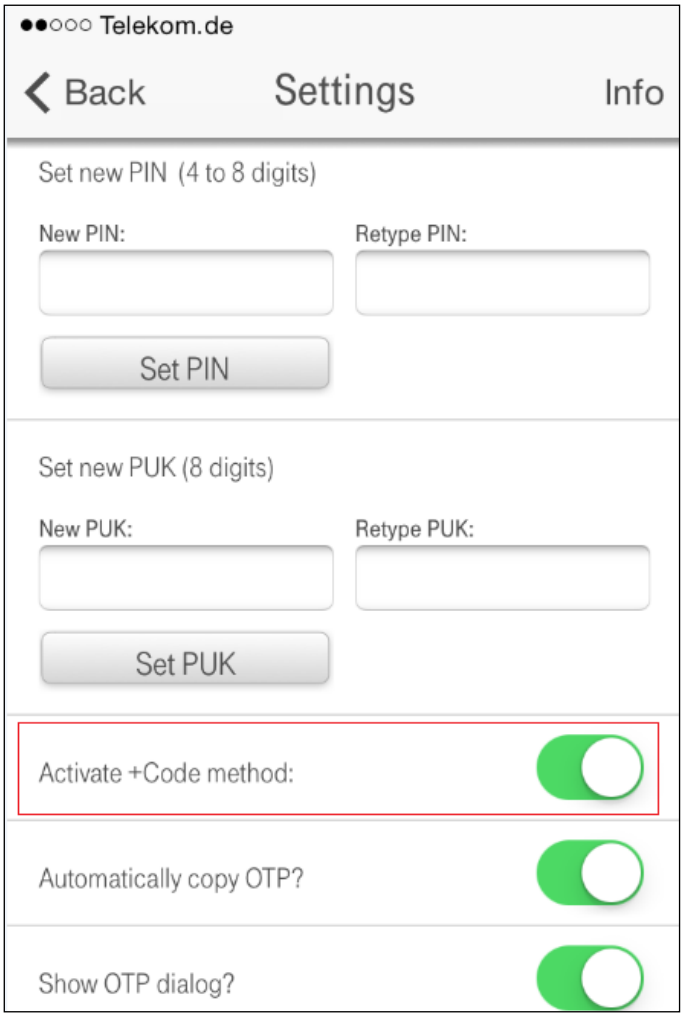



Figure 9: Settings menu

After you have returned to the main view using the “Back” button, an additional entry field appears, in which you have to enter the required code (displayed on your log-in screen) before generating the next one-time password is triggered.

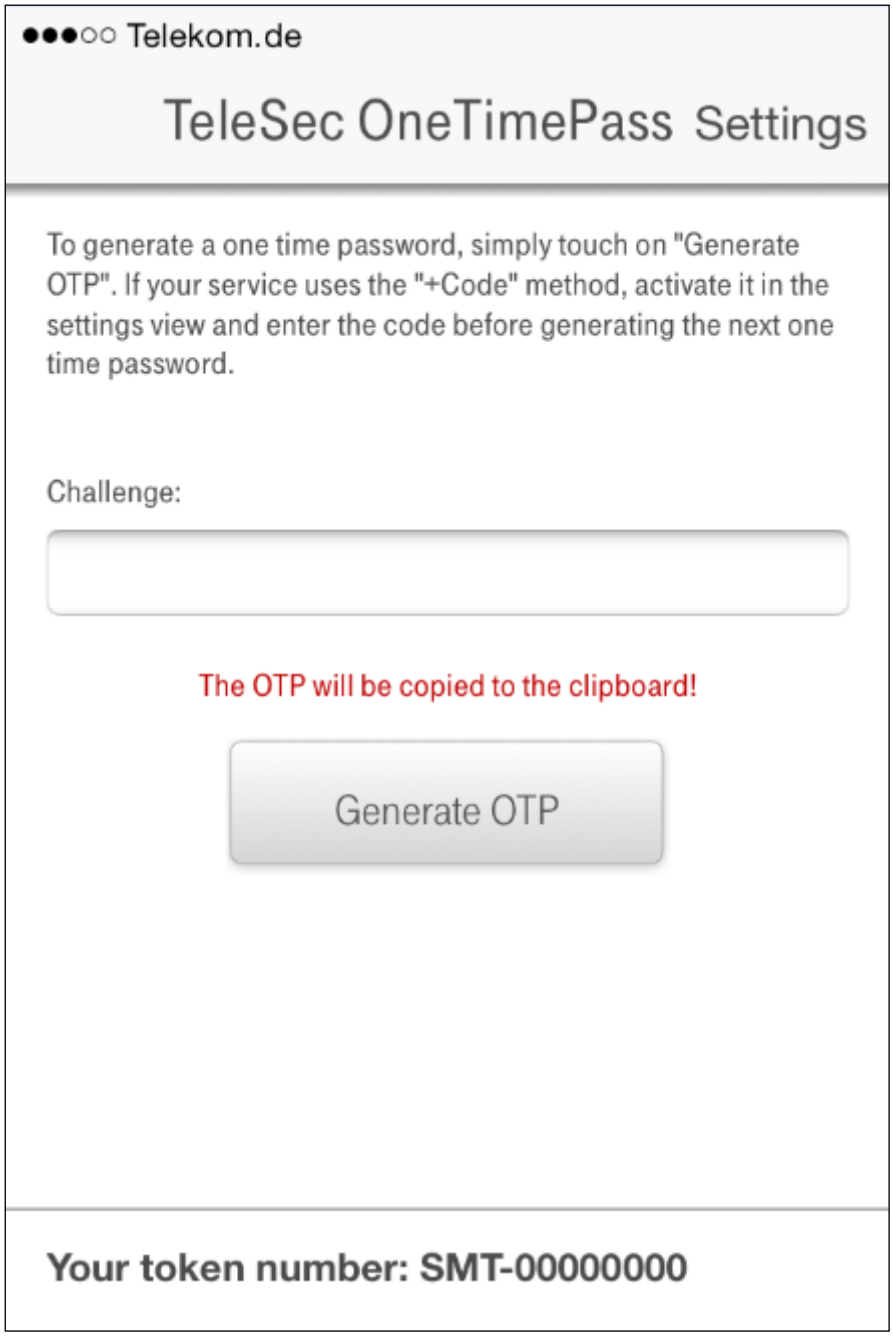



Figure 10: One-time password generation using „+Code“-procedure

After entering the code, you are able to generate the OTP as usual by touching the “Generate OTP” button.

Every time you leave the app, whether by touching the Home button or the Block button, switching to a phone call or going to another app, you then have to reactivate the Smart-Token using the PIN you assigned during activation the next time you use the application.

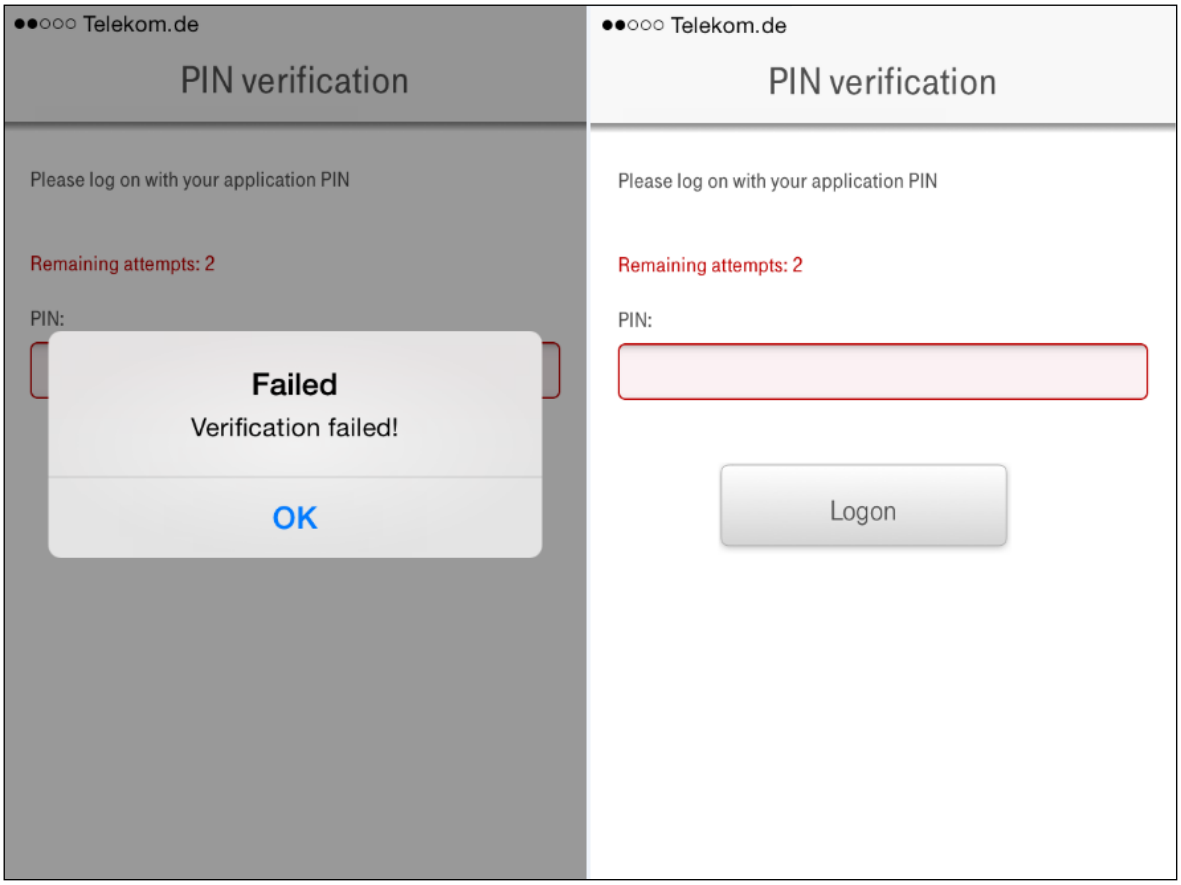



Figure 11: PIN-entry / failed attempts

If you mistype the PIN during entry, a dialog informs you of this and the failed logon attempts counter is reduced accordingly. The remaining attempts are displayed above the PIN field in red text.

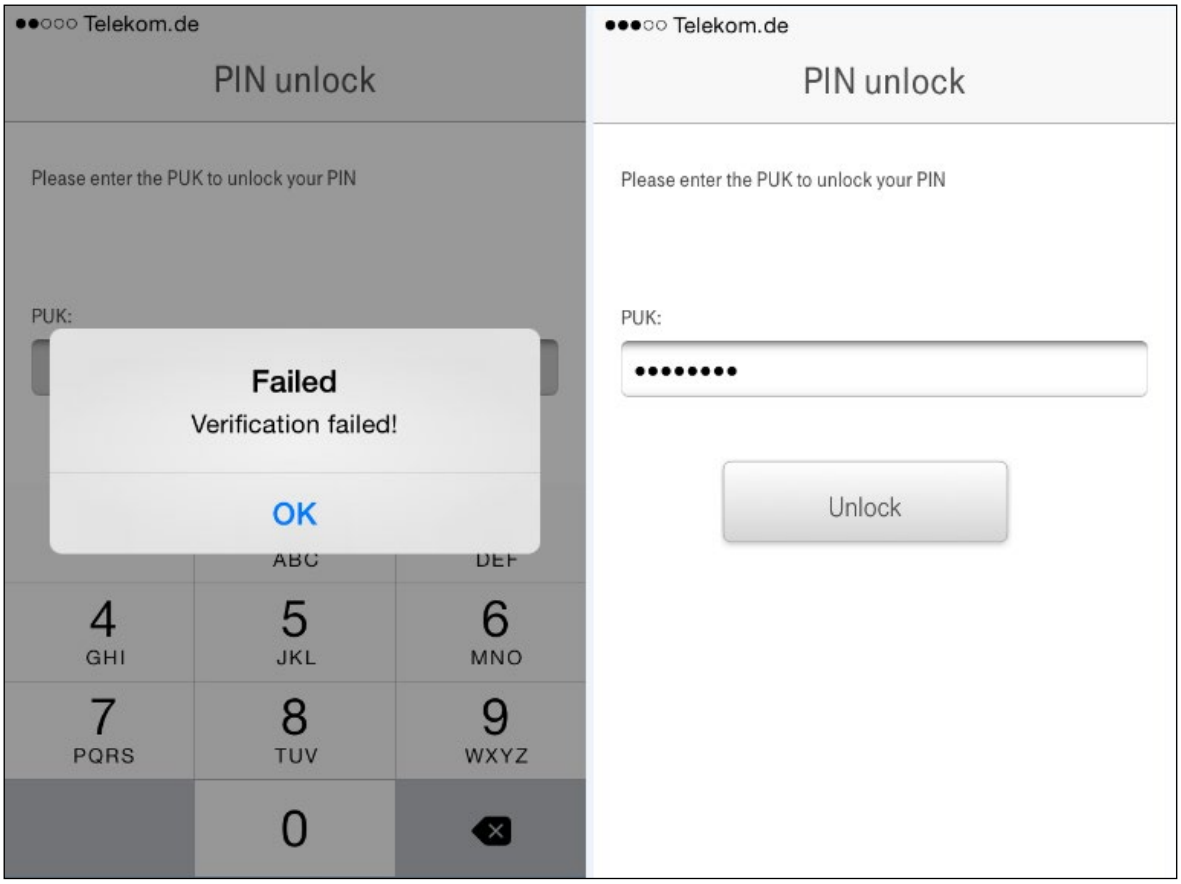



Figure 12: Incorrect PIN entry

If you have entered an incorrect PIN three times in a row, the application is initially blocked. However, you can unblock the PIN using the PUK, which you have also assigned during the activation.

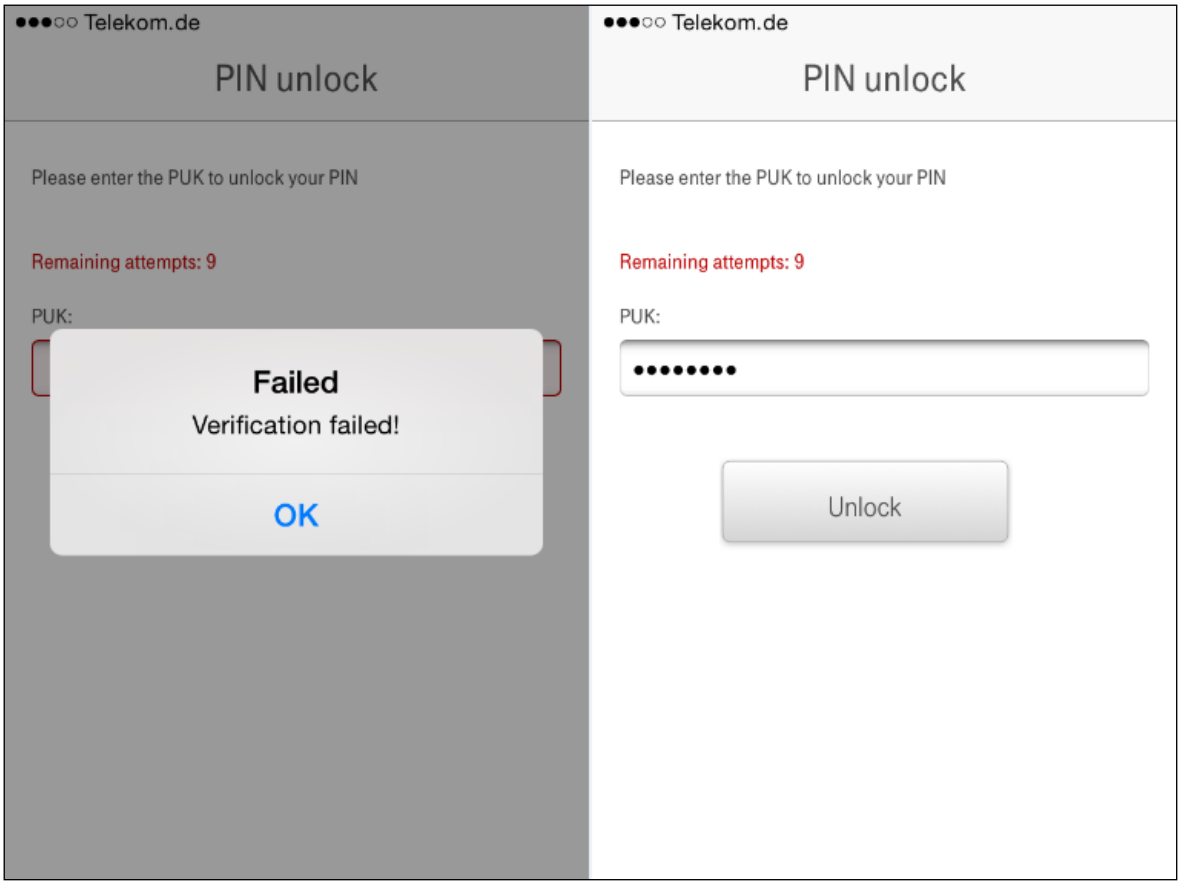



Figure 13: Unblocking the PIN with the PUK

The form for entering the PUK is automatically displayed, if the failed logon attempt counter has run out. After you have unblocked the app by entering the correct PUK, you can continue to use it as normal.

# 6 CHANGING PIN OR PUK

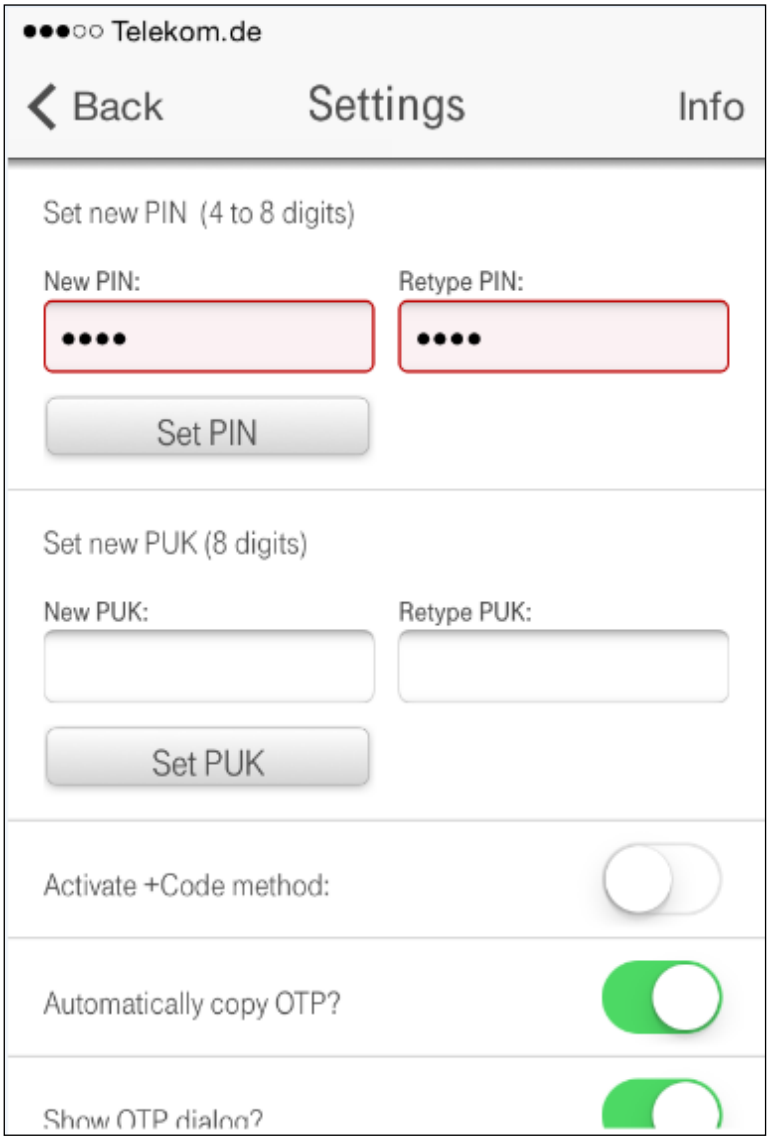



Figure 14: Settings: change PIN/PUK

Except activation of the “+Code” procedure (see Section 5.2), the settings menu allows you to change both the PIN and the PUK. You do not need to enter your current PIN as you have to log on successfully to the Smart-Token using your PIN before you can access the Settings menu.

⚠ Please note that the PIN must contain 4-8 digits and the PUK 8 digits.

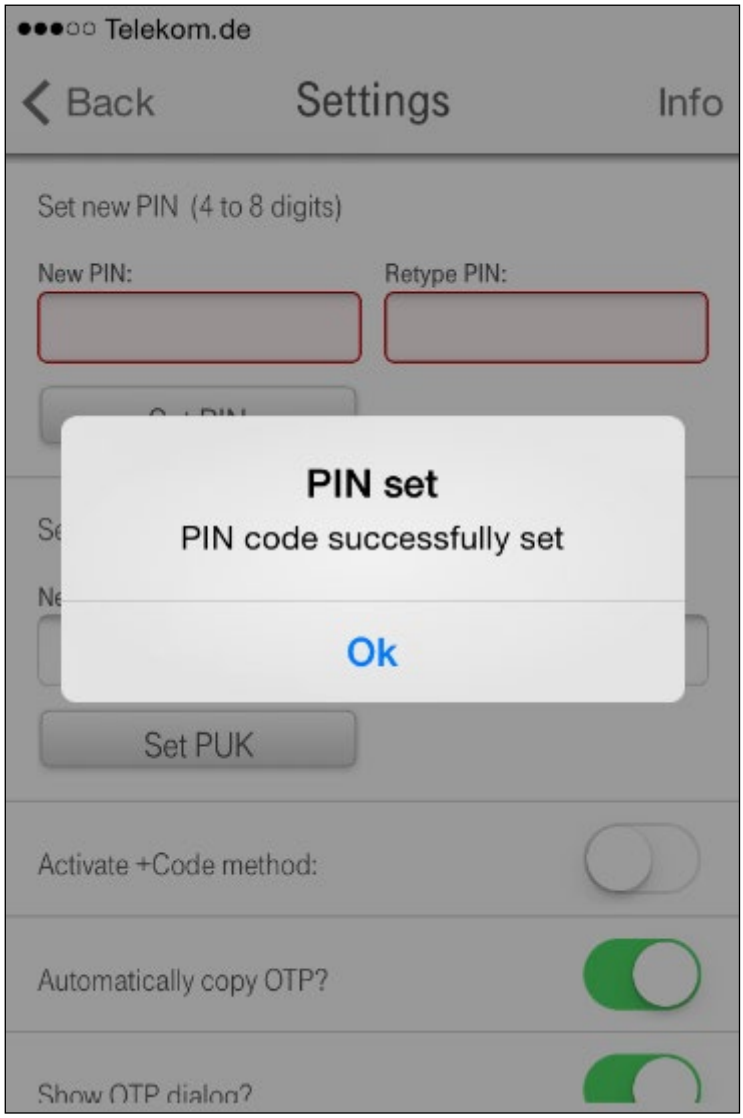



Figure 15: PIN changed successfully

After entering a new PIN or PUK twice, you simply have to touch the “Set PIN/Set PUK” button. After the PIN/PUK has been changed successfully, the corresponding success notification appears on the screen.

# 7 FORGOTTEN PIN OR PUK

If you have entered an incorrect PIN three times in a row, the app automatically requests the PUK that you defined during installation.
If you also enter this PUK incorrectly ten times in a row, we have to assume misuse and the app is automatically reset. All secrets are then deleted and the OneTimePass.ID Smart-Token app has to be reactivated.

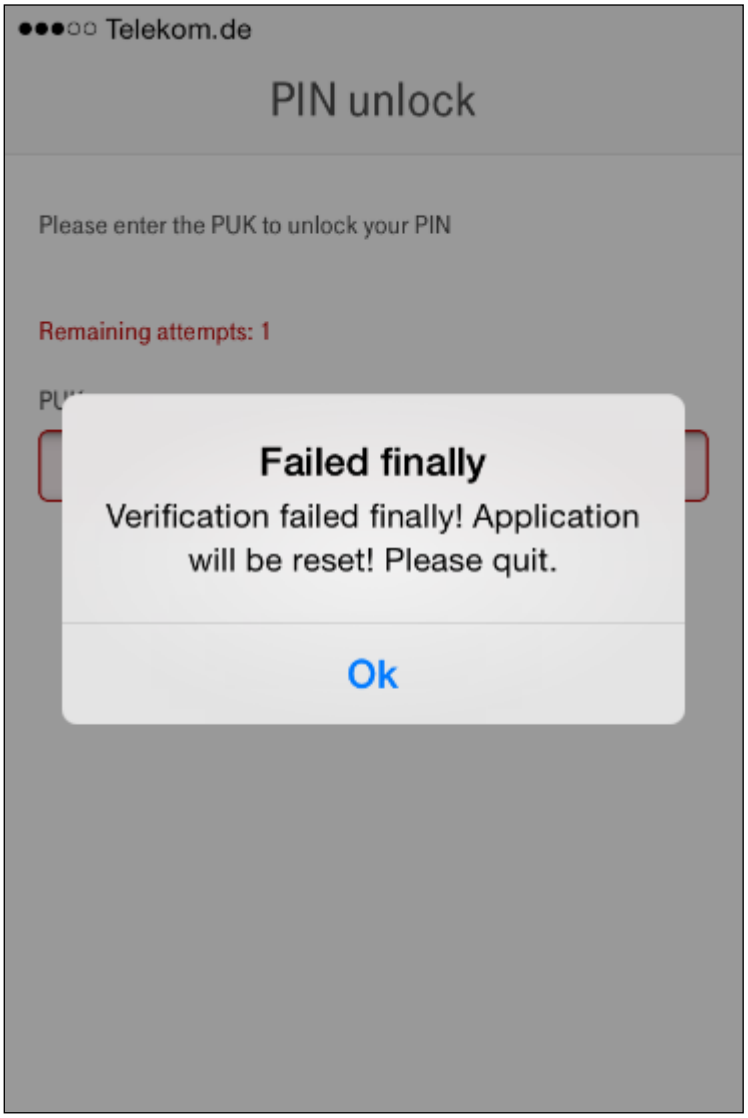



Figure 16: Reset Smart-Token

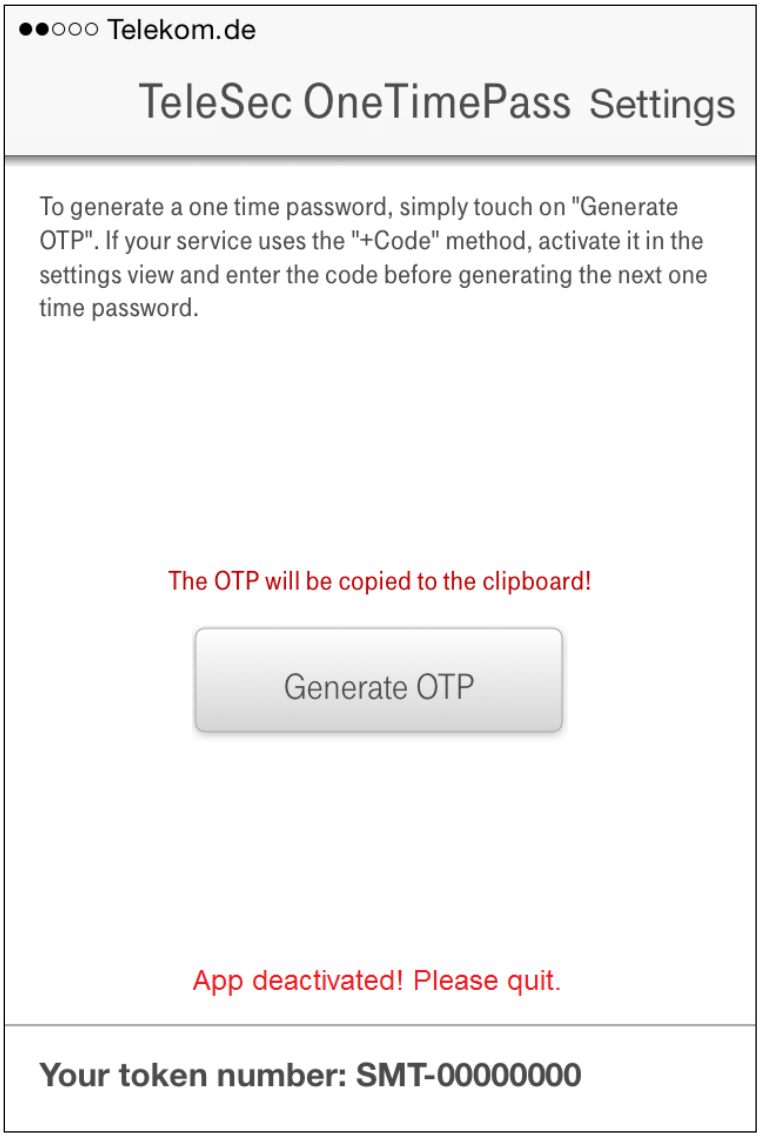



Figure 17: Request to close the app

# 8 RE-INITIALIZATION

To perform a re-initialization, enter the token number that you were given when activating the Smart-Token. The token number is also displayed each time after entering the PIN. If you do not remember the token number, please contact the OneTimePass.ID Administrator (within your organization), who is responsible for your organization.

For a successful re-initialization, you need an internet connection via wireless LAN or via your mobile network provider.

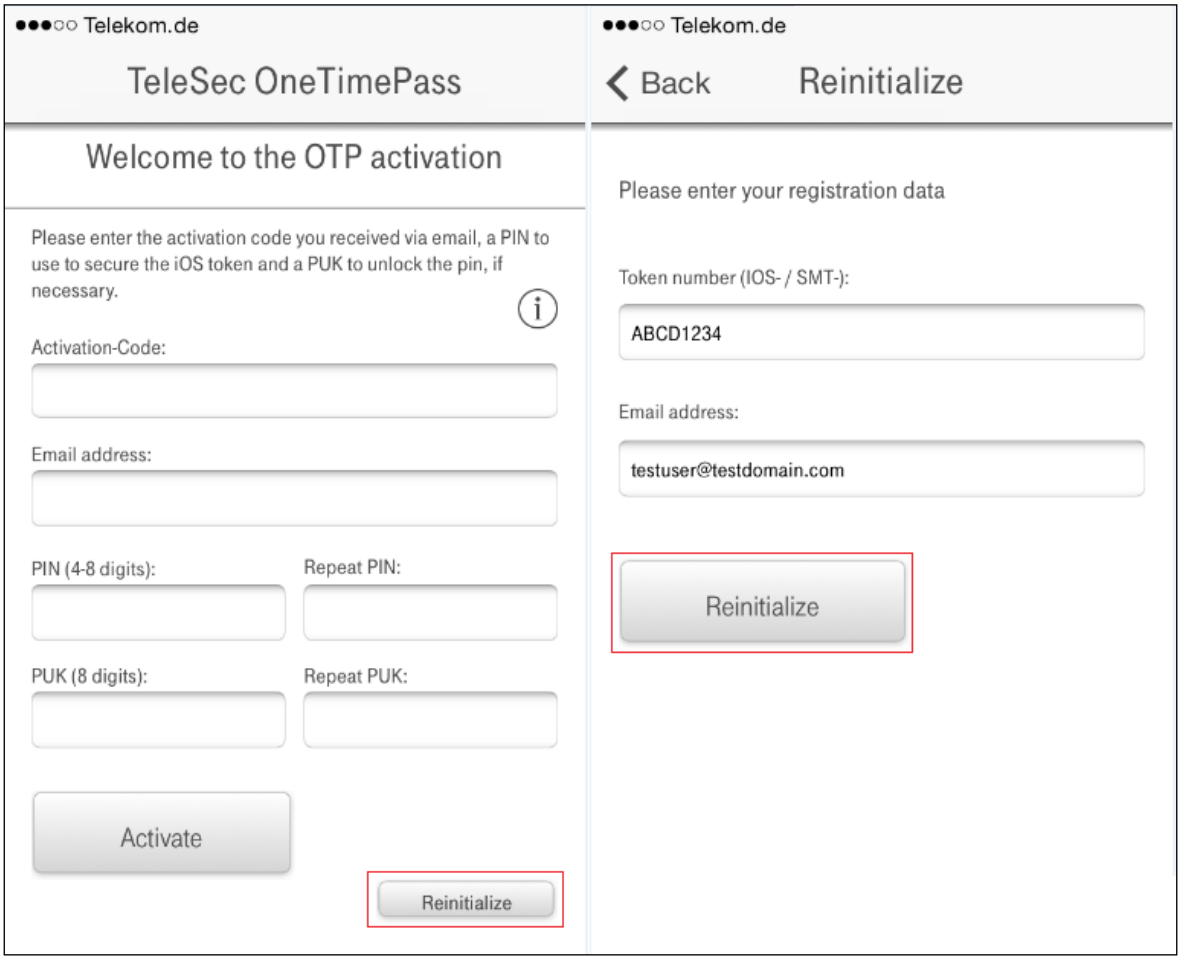



Figure 18: Re-initialization

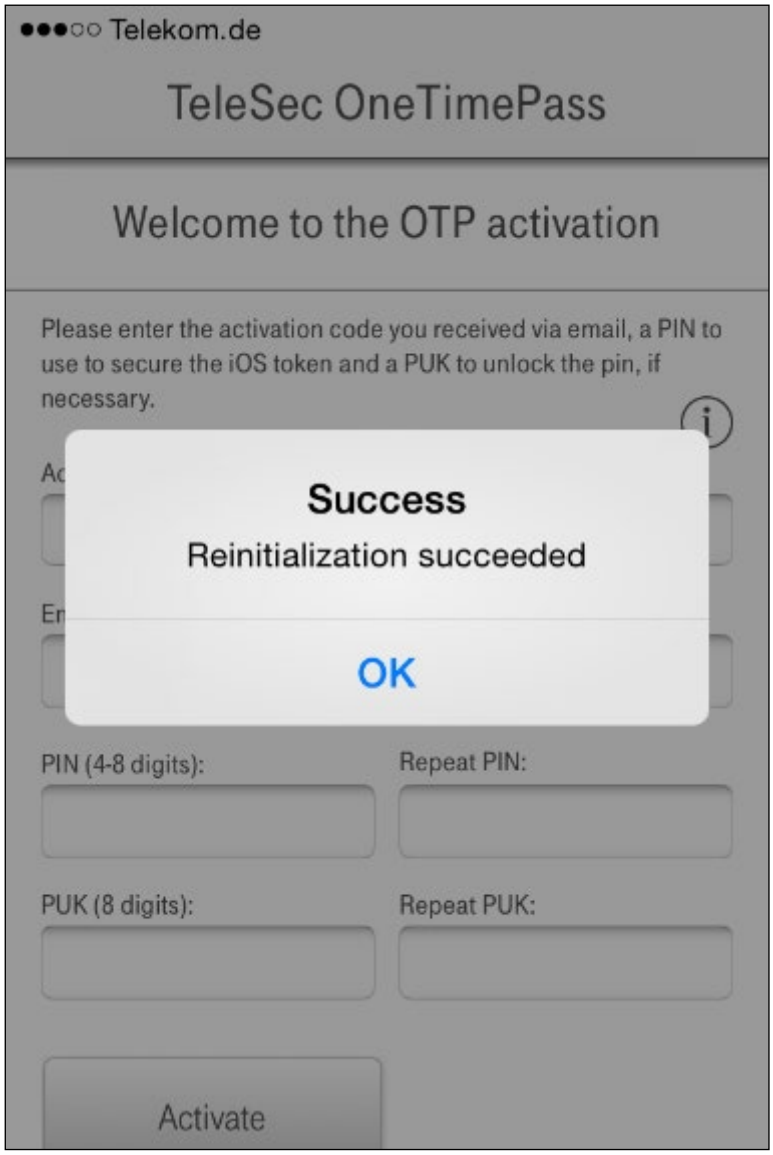



Figure 19: Successful Re-initialization

After starting the re-initialization, you will receive a new activation code for your Smart-Token via email.

Sehr geehrte Kundin, sehr geehrter Kunde,

für Ihren OneTimePass-Software-Token wurde soeben eine Reaktivierungs-Anfrage gesendet.

Mit dem folgenden Aktivierungs-Code können Sie die Initialisierung erneut durchführen:

Aktivierungs-Code : abcde1234

Bitte verwenden Sie Ihren Software-Token wie im Handbuch beschrieben.

Um OneTimePass in vollem Umfang nutzen zu können, ist die Definition eines Servicepasswortes erforderlich.
Hierzu melden Sie sich bitte als User mit Ihrer Tokennummer und einem gültigen OneTimePasswort an der
Benutzeroberfläche der OneTimePass Internetseite an (https://onetimepass.telesec.de).
Wählen Sie im Menü den Punkt "Servicepasswort". Hier können Sie ein individuelles Servicepasswort festlegen.

-
- Bitte antworten Sie nicht auf diese EMail. Sollten Sie Fragen haben oder
- Informationen benötigen, wenden Sie sich bitte an Ihren Provider.
-

---

Dear customer,

Your OneTimePass SmartToken has been created by your administration service.

Please follow your User Guide to complete the initialisation procedure.
You will need to use the following activation code during the initialisation procedure:

activation code : abcd1234

If you are unsure how to use the SmartToken please refer to the User Guide for further details.
For additional information or any questions please contact your service desk.

To use OneTimePass in its entirety the definition of a service password is needed.
For this please log on as user to the service web sites (https://onetimepass.telesec.de) with your toke number and a valid one time password.
Choose the menu point "service password". There you can set an individual service password.

Please do not reply to this message.

Figure 20: Re-Initialization email

The procedure for continuing the re-initialization is similar to the activation process (see Section 4).

# 9 CONTACT FOR FURTHER QUESTIONS

For further questions you can contact the OneTimePass.ID Administrator (within your organization), who is responsible for your organization.

# 10 LIST OF FIGURES

Figure 1: Initial screen ..... 5
Figure 2: Smart-Token app on Apple iTunes Store ..... 6
Figure 3: Activation email ..... 7
Figure 4: Activation screen ..... 8
Figure 5 Entering PIN and PUK ..... 9
Figure 6: Successful activation ..... 10
Figure 7: Start screen of the ready-to-use SmartToken ..... 11
Figure 8: Generated one-time password in the OTP-Dialog & OTP-Settings ..... 12
Figure 9: Settings menu ..... 13
Figure 10: One-time password generation using „+Code“-procedure ..... 14
Figure 11: PIN-entry / failed attempts ..... 15
Figure 12: Incorrect PIN entry ..... 16
Figure 13: Unblocking the PIN with the PUK ..... 17
Figure 14: Settings: change PIN/PUK ..... 18
Figure 15: PIN changed successfully ..... 19
Figure 16: Reset Smart-Token ..... 20
Figure 17: Request to close the app ..... 21
Figure 18: Re-initialization ..... 22
Figure 19: Successful Re-initialization ..... 23
Figure 20: Re-Initialization email ..... 24