



# DB Secure Authenticator (DBSA)

## User Guide

Version 1.0  
April 2025

# DBSA User Guide

Last Update, April 2025

## Table of Contents

- 1.0 Description of the Service ..... 5
- 1.1 DBSA Availability ..... 5
- 1.2 DBSA and Strong Customer Authentication ..... 5
- 2.0 Downloading / Procuring DBSA Token ..... 6
- 2.1 Downloading DBSA Mobile Application ..... 6
- 2.2 Ordering a DBSA Physical Token ..... 6
- 3.0 Activating your DBSA Mobile App ..... 7
- 3.1 Open the app and accept the terms and conditions displayed. .... 7
- 3.2 Create a PIN for your device. .... 7
- 3.3 Log into Autobahn to Register Security Device ..... 8
- 3.4 Click Activate Token ..... 9
- 3.5 Scan First QR-Code and Input First Activation Code ..... 9
- 3.6 Confirm Scanning of First QR Code ..... 11
- 3.7 Receive and Scan 2<sup>nd</sup> QR-Code and Input 2<sup>nd</sup> Activation Code ..... 11
- 3.8 Confirm Scanning of Second QR Code ..... 12
- 3.9 Complete your device registration. .... 13
- 4.0 Activating your DBSA Hardware Token ..... 14
- 4.1 Unpack the device ..... 14
- 4.2 Set the device’s language. .... 14
- 4.3 Set the device’s PIN ..... 15
- 4.4 Log into Autobahn to Register Security Device ..... 16
- 4.5 Click Activate Token ..... 17
- 4.6 Scan First QR-Code and Input First Activation Code ..... 17
- 4.7 Confirm Scanning of First QR Code ..... 18

- 4.8 Receive and Scan 2<sup>nd</sup> QR-Code and Input 2<sup>nd</sup> Activation Code .....19
- 4.9 Complete your device registration .....20
- 5.0 DBSA Functionalities and Capabilities .....21
- 5.1 Scanning QR Codes – Prerequisite of at least one active token .....21
- 5.2 Logging in with DB Secure Authenticator (After Activation) .....22
- 6.0 DBSA Settings (For mobile application) .....25
- 6.1 Change DBSA Login PIN – for mobile app.....25
- 6.2 Activate multiple soft tokens. ....26
- 6.3 Change Token ID name in case of multiple tokens (mobile app).....28
- 6.4 Delete an activated token. ....28
- 7.0 DBSA Settings (For hardware device) .....29
- 7.1 Enter Settings .....29
- 7.2 Select Language .....29
- 7.3 Change Device PIN .....30
- 7.4 Delete Active Token.....31
- 8.0 Reset your DB Secure Authenticator .....32
- 8.1. Go to Autobahn and click “Reset DB Secure Authenticator” .....32
- 8.2. Provide your username to receive reset confirmation .....32
- 8.3. Confirm the reset of the DB Secure Authenticator .....33
- 8.4. Deactivate your actual tokens (software or hardware).....33
- 8.5. Re-activate your actual tokens (software or hardware).....33

Version	Version Date	Reason for new Version
<b>1.0</b>	01.04.2025	A refreshed user guide combining all existing DBSA user guides,

## 1.0 Description of the Service

The DB Secure Authenticator (DBSA) is an authentication token available as a hardware or mobile application (iOS and Android) that allows users to securely log-in and authorise instructions and transactions.

Using the DBSA, users can log-in by scanning the QR code that generates a One-Time-Password on the device, or by generating an OTP directly after inserting the 6-digit PIN.

To authorise a transaction, DBSA uses the device's camera to scan the transaction details displayed online as a cryptographic QR code. The app then displays the respective OTP to sign the specific transaction.

This ensures the highest level of security and is aligned to the dynamic linking regulation under the Payment Services Directive II in Europe and to "You Sign What You See" in Asia.

## 1.1 DBSA Availability

DBSA is available as:

- Soft Token (e.g., mobile app available on iOS and Android)
  - Available everywhere with the exception being Android in China
- Hard Token (e.g., hardware device like DigiPass 770R)
  - Not offered in China.

## 1.2 DBSA and Strong Customer Authentication

Strong means of authentication are required to ensure that only the entitled individual can retrieve information, initiate or authorise a transaction on specific Deutsche Bank accounts.

Strong customer authentication is one of the main pillars in the overall fraud prevention and detection strategy as ultimately any other controls circle around and back to it in order to verify the identity and original intent of an authorised banking partner. It is also a global theme in a regulatory context whether it is in Asia where it is referred to as Two Factor Authentication, the Americas where it is referred to as Multiple Factor Authentication, or Europe where it is referred to as Strong Customer Authentication.

The concept is always the same in that an authentication is considered strong enough as long as it builds up on two separate elements being either possession (e.g., a token, an app, a smartcard), knowledge (e.g., PIN, password), or inherence (e.g., biometrics).

## 2.0 Downloading / Procuring DBSA Token

In order to use the DB Secure Authenticator, you will need to download the soft (mobile) version or order the physical device.

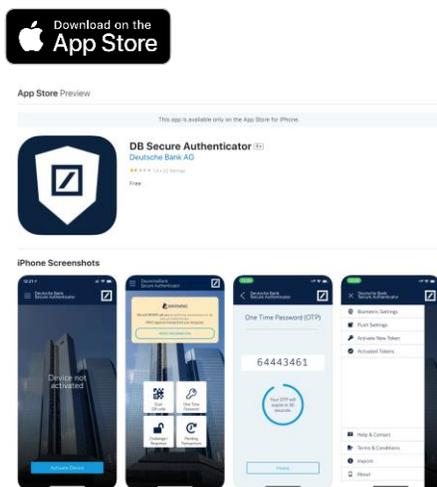
### 2.1 Downloading DBSA Mobile Application

To download the DB Secure Authenticator mobile app, proceed to your App Store of choice:

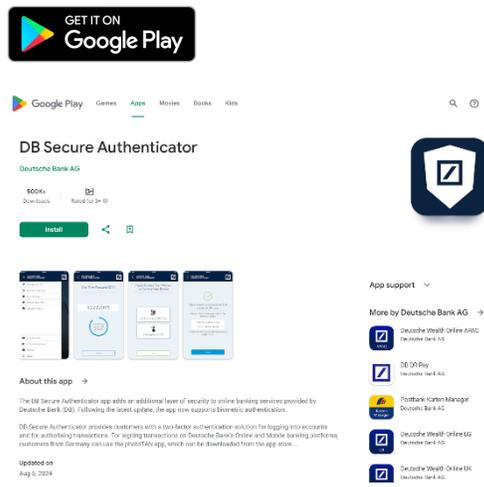
1. iOS App Store
2. Google Play Store

Search for “DB Secure Authenticator” and install the application.

#### Apple App Store



#### Google Play Store



### 2.2 Ordering a DBSA Physical Token

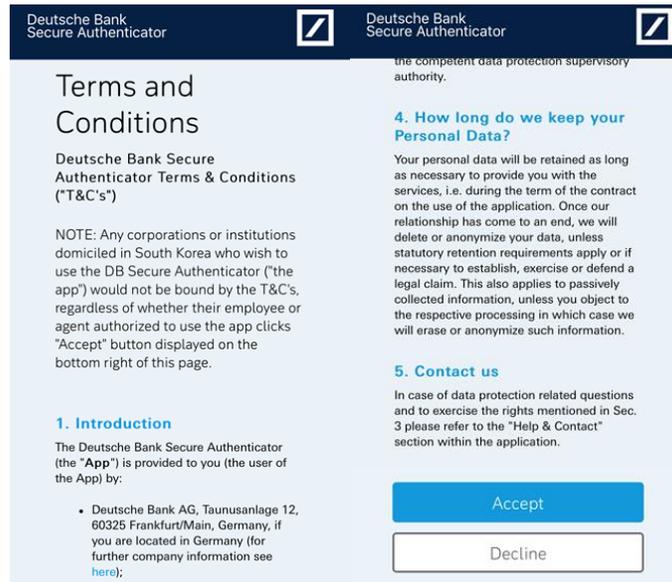


To order the DB Secure Authenticator Physical Token, please either:

1. Reach out to your Deutsche Bank contact; or
2. Access the Genostore Webshop at <https://genostore.de/dbco/> to order the token.

### 3.0 Activating your DBSA Mobile App

#### 3.1 Open the app and accept the terms and conditions displayed.



#### 3.2 Create a PIN for your device.

- Create and confirm your 6 Digit PIN.



### 3.3 Log into Autobahn to Register Security Device

This step requires you to log into Autobahn to register your DB Secure Authenticator.

Request Access

Autobahn

\* Username: newdbsetup@test.com  
 Remember my Username

\* Password: [masked]  
[Clear]

Login Mode: Password

Language: English

Submit Clear Form

**Cyber Fraud Prevention**

Deutsche Bank has established a comprehensive information and cyber security program with a high standard financial industry security governance framework and organization to implement control and adherence to security policies and standards in conjunction with evolving business requirements, regulatory guidance and an emerging threat landscape.

Nevertheless it's important that you protect yourself by understanding the evolving fraud schemes and that you follow the best practices to mitigate internet payment fraud.

Reset DB Secure Authenticator  
Order DB Secure Authenticator  
Forgot Password?  
**Register Security Device**  
Self-Diagnostic tool  
Download  
Security Awareness

**Unauthorised Access Warning:** Access to this service is prohibited unless authorised. Accessing programs or data unrelated to your job is prohibited.

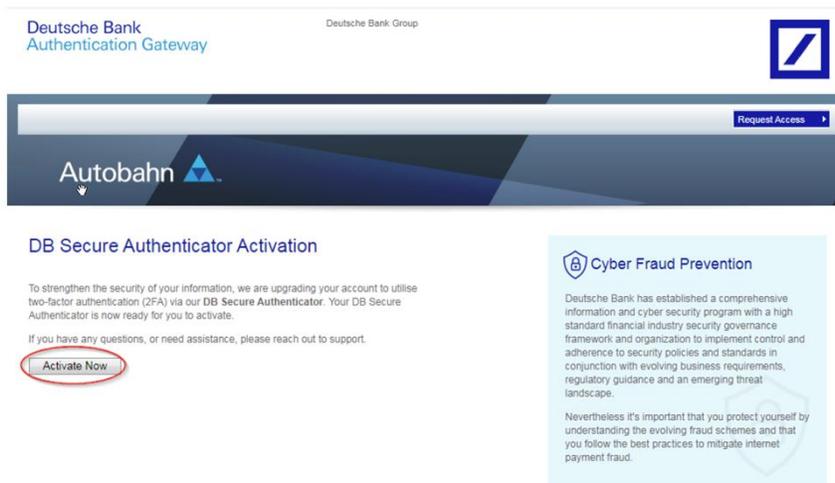
Disclaimer & Privacy Policy | Cookie Notice | Cyber Fraud Prevention  
Copyright © 2020 Deutsche Bank AG, Frankfurt am Main

- Click “Register Security Device”
- Enter your username and password\*

\*If this is the first time you are logging into Autobahn, you will need to insert your initial one-time login password.

As a part of your user set up, you would have received a welcome email with an **encrypted PDF** that contains the one-time credentials. To obtain the PIN to unlock the encrypted PDF, it has been sent to your colleague or Deutsche Bank service team (please refer to that email). Please reach out accordingly to them to obtain the PIN to then get your one-time login credentials.

### 3.4 Click Activate Token

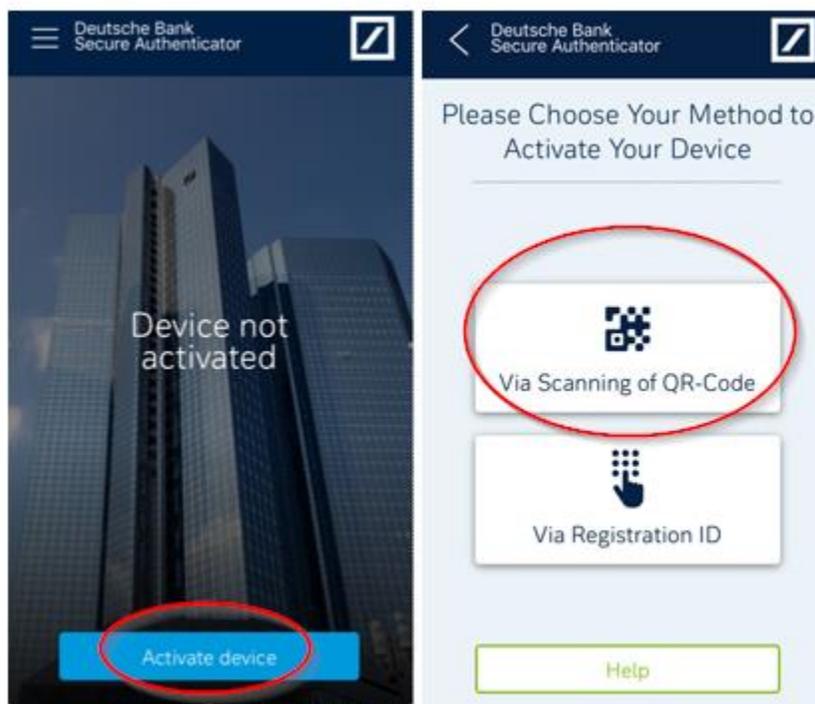


### 3.5 Scan First QR-Code and Input First Activation Code

You will now see a QR code on the screen.

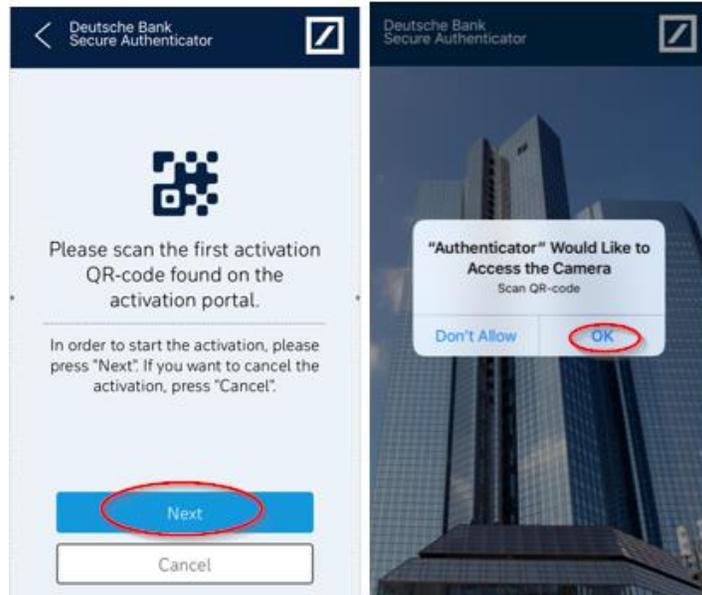
Go to your **DB Secure Authenticator**

- Click “Activate Device”
- Click “Via Scanning of QR Code”

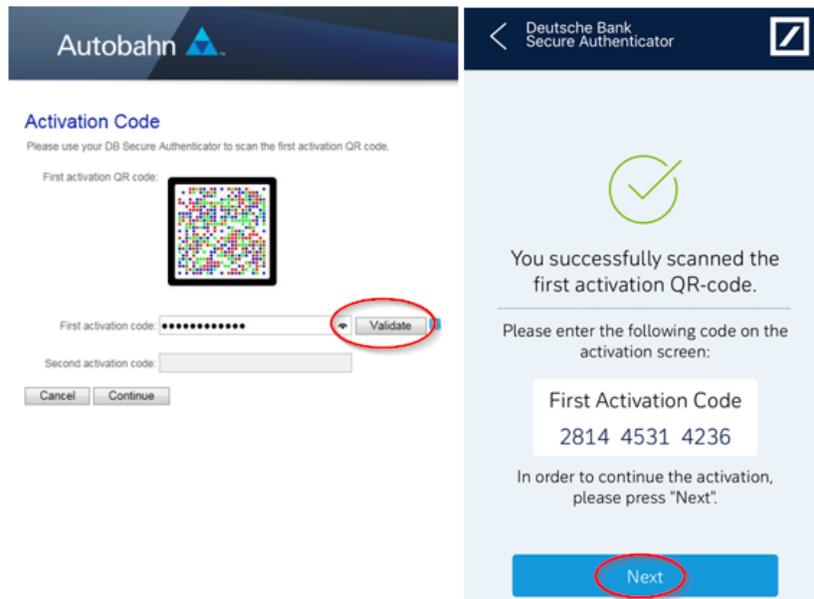


Refer to the next page for continued instructions for 3.5.

- Click “Next”
- Click “OK” to allow the app to utilise its camera



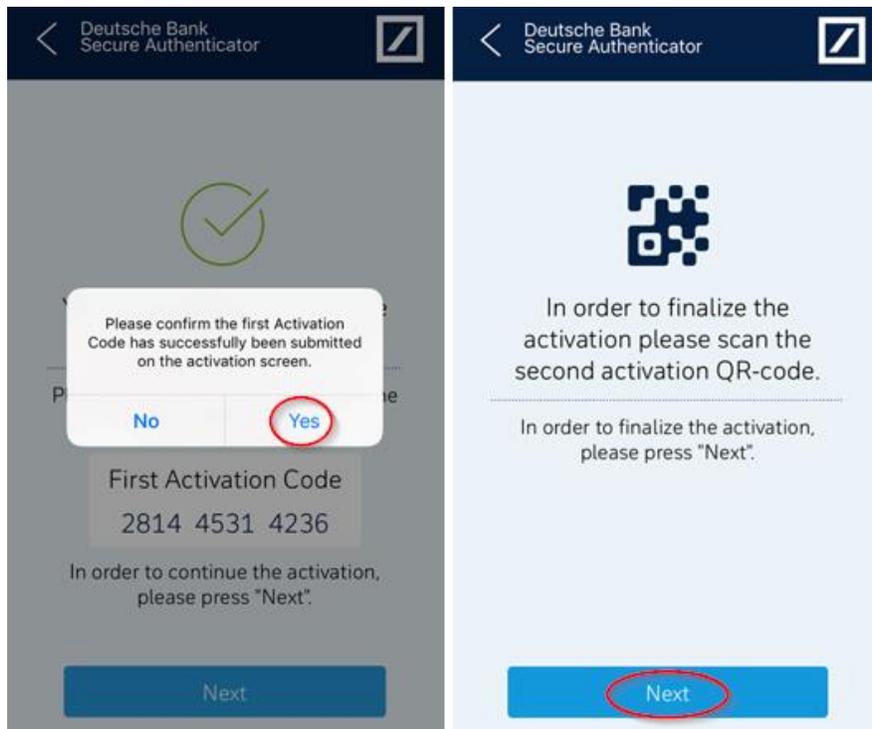
- Using the DB Secure Authenticator, scan the first QR code displayed on the device launching Autobahn.
- After scanning the first QR code, you will receive a code on your DBSA device.
- Input the abovementioned code into the first activation code field.
- Click “Validate” on the device launching Autobahn.
- Press “Next” on your DBSA device.



### 3.6 Confirm Scanning of First QR Code

On your DB Secure Authenticator device:

- Click “Yes” to confirm.
- Press “Next” to proceed.



### 3.7 Receive and Scan 2<sup>nd</sup> QR-Code and Input 2<sup>nd</sup> Activation Code



Dear User

You are in the process of activating your DB Secure Authenticator.

This is the second activation QR-code to complete the activation.



Please follow the steps below

1. Please scan the code with your DB Secure Authenticator.
2. A 7 digit activation code will be generated on the token.

Please enter the same against 'Second activation code' field on your activation screen to proceed further.

**Please note:**

If your DB Secure Authenticator has timed-out/turned off by the time you receive this email,

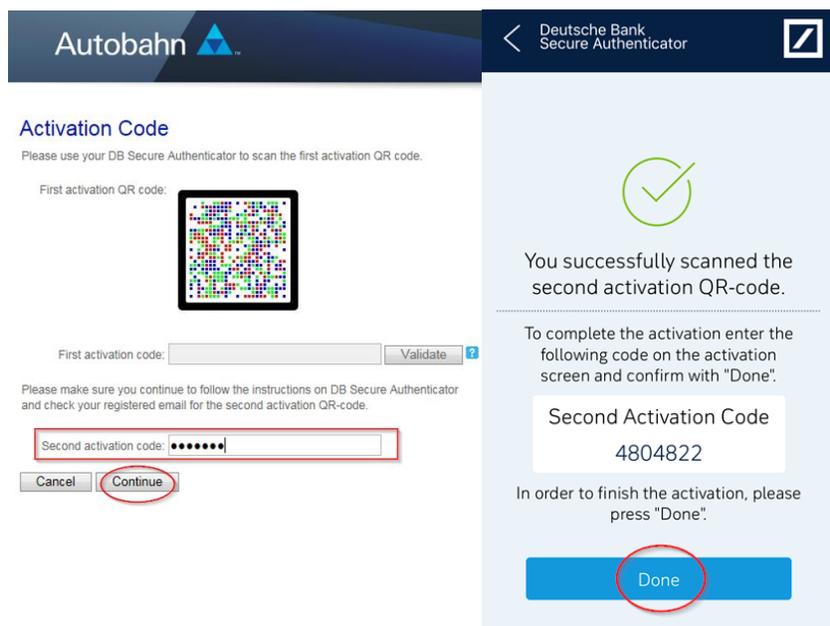
DB Secure Authenticator will ask for the first QR-code again, once it is turned back on. In this case to complete the activation please:

- Scan the first QR-code again, which is still displayed on the activation screen
- Follow the instructions on the DB Secure Authenticator and scan the second QR-code from this mail

- You will receive an email containing the second QR-Code (sender: [db-direct.alerts@db.com](mailto:db-direct.alerts@db.com))
- Using your DB Secure Authenticator, scan the second QR code.

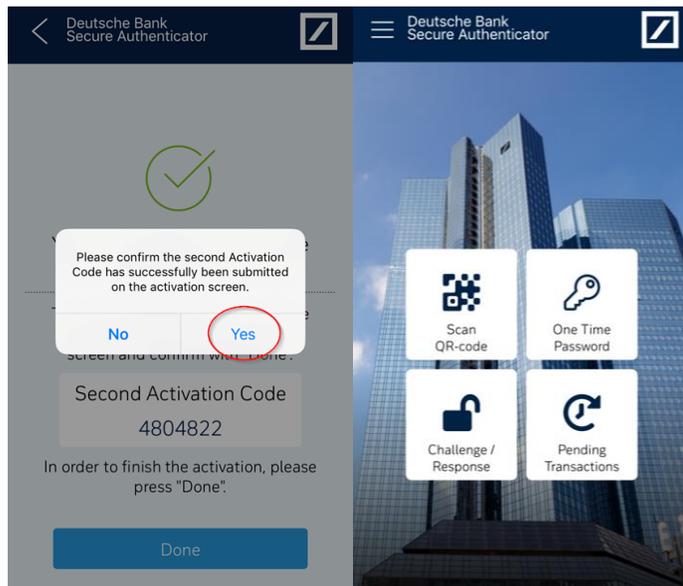
Refer to the next page for continued instructions for 3.7.

- Insert the second activation code into the second activation code field.
- Click “Continue” on the device launching Autobahn.
- Press “Done” on your DB Secure Authenticator.



### 3.8 Confirm Scanning of Second QR Code

- Click “Yes” on your DB Secure Authenticator to finish.
- The DBSA home page will appear.



### 3.9 Complete your device registration.

- Click complete on your device launching Autobahn.
- Wait for 30 minutes before logging back in.

## 4.0 Activating your DBSA Hardware Token

### 4.1 Unpack the device.

- Insert batteries into the DBSA Hardware Token.
- Switch on the device by pressing the orange button with the POWER button.



### 4.2 Set the device's language.

- Scroll to select the language.
- Confirm the language selection.



### 4.3 Set the device's PIN

- Click “Continue” to create PIN.
- Enter desired PIN.
- Confirm desired PIN.
- Click “Continue” to acknowledge.



## 4.4 Log into Autobahn to Register Security Device

This step requires you to log into Autobahn to register your DB Secure Authenticator.

Request Access

Autobahn

\* Username:   Remember my Username ?

\* Password:

Login Mode:

Language:

**Cyber Fraud Prevention**

Deutsche Bank has established a comprehensive information and cyber security program with a high standard financial industry security governance framework and organization to implement control and adherence to security policies and standards in conjunction with evolving business requirements, regulatory guidance and an emerging threat landscape.

Nevertheless it's important that you protect yourself by understanding the evolving fraud schemes and that you follow the best practices to mitigate internet payment fraud.

[Reset DB Secure Authenticator](#)  
[Order DB Secure Authenticator](#)  
[Forgot Password?](#)  
**[Register Security Device](#)**  
[Self-Diagnostic Tool](#)  
[Download](#)  
[Security Awareness](#)

**Unauthorised Access Warning:** Access to this service is prohibited unless authorised. Accessing programs or data unrelated to your job is prohibited.

[Disclaimer & Privacy Policy](#) | [Cookie Notice](#) | [Cyber Fraud Prevention](#)  
Copyright © 2020 Deutsche Bank AG, Frankfurt am Main

- Click “Register Security Device”
- Enter your username and password\*

\*If this is the first time you are logging into Autobahn, you will need to insert your initial one-time login password. This can be obtained in two ways depending on your user set up:

As a part of your user set up, you would have received a welcome email with an **encrypted PDF** that contains the one-time credentials. To obtain the PIN to unlock the encrypted PDF, it has been sent to your colleague or Deutsche Bank service team (please refer to that email). Please reach out accordingly to them to obtain the PIN to then get your one-time login credentials.

## 4.5 Click Activate Token

On your device with Autobahn launched, click “Activate Token”

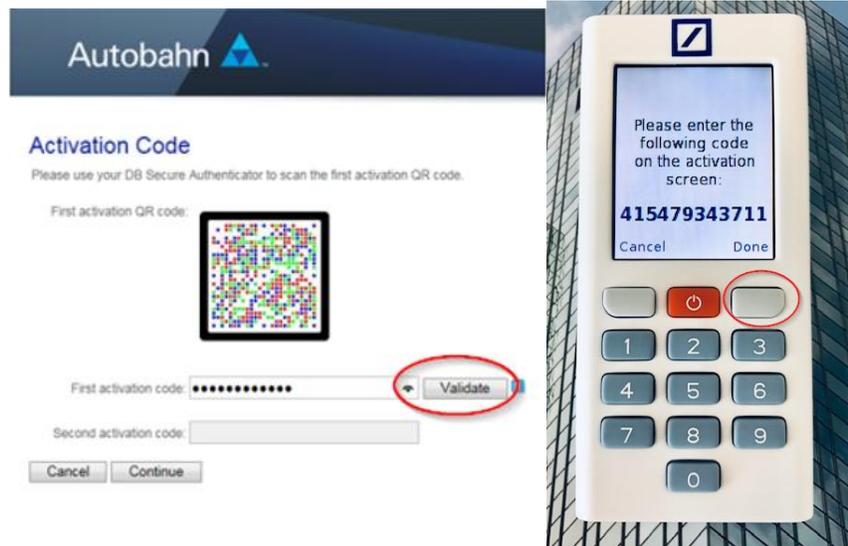


## 4.6 Scan First QR-Code and Input First Activation Code

- Using the DB Secure Authenticator, click “continue”.
- The camera functionality will open.



- Using the DB Secure Authenticator, scan the first QR code displayed on the device launching Autobahn.
- After scanning the first QR code, you will receive a code on your DBSA device.
- Input the abovementioned code into the first activation code field.
- Click “Validate” on the device launching Autobahn.
- Press “Next” on your DBSA device.



#### 4.7 Confirm Scanning of First QR Code

On your DB Secure Authenticator device:

- Click “Yes” to confirm.
- Press “Continue” to proceed.



## 4.8 Receive and Scan 2<sup>nd</sup> QR-Code and Input 2<sup>nd</sup> Activation Code



Dear User

You are in the process of activating your DB Secure Authenticator.

This is the second activation QR-code to complete the activation.



Please follow the steps below

1. Please scan the code with your DB Secure Authenticator.
2. A 7 digit activation code will be generated on the token.

Please enter the same against 'Second activation code' field on your activation screen to proceed further.

**Please note:**

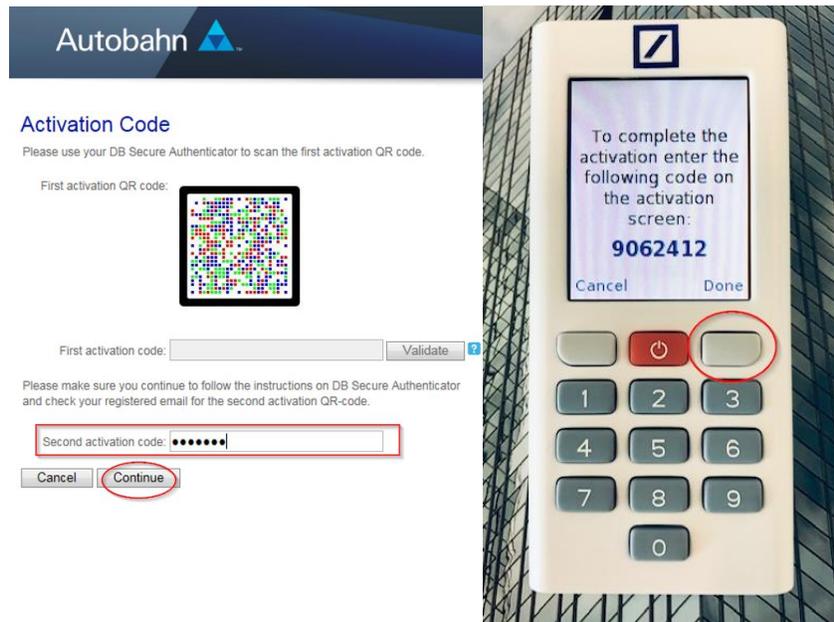
If your DB Secure Authenticator has timed-out/turned off by the time you receive this email,

DB Secure Authenticator will ask for the first QR-code again, once it is turned back on. In this case to complete the activation please:

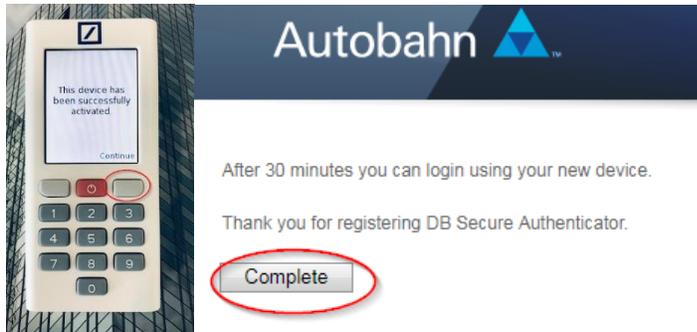
- Scan the first QR-code again, which is still displayed on the activation screen
- Follow the instructions on the DB Secure Authenticator and scan the second QR-code from this mail

- You will receive an email containing the second QR-Code (sender: [db-direct.alerts@db.com](mailto:db-direct.alerts@db.com))
- Using your DB Secure Authenticator, scan the second QR code.

- Insert the second activation code into the second activation code field.
- Click “Continue” on the device launching Autobahn.
- Press “Done” on your DB Secure Authenticator.



#### 4.9 Complete your device registration



- Click complete on your device launching Autobahn.
- Wait for 30 minutes before logging back in.

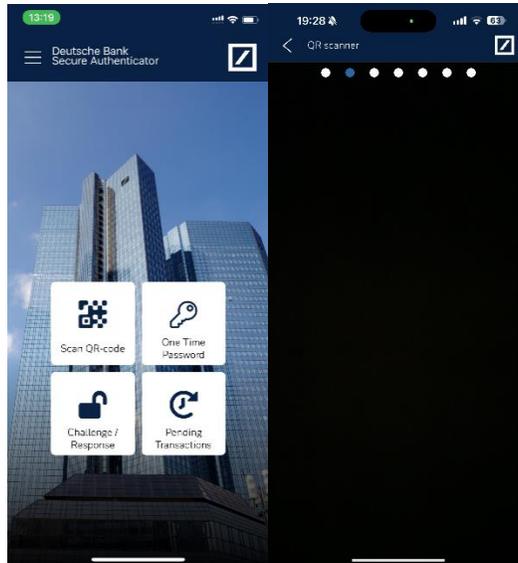
## 5.0 DBSA Functionalities and Capabilities

### 5.1 Scanning QR Codes – Prerequisite of at least one active token

When scanning a QR code, the client should hold the device upright in front of the QR image to enable QR scanning.

For mobile app:

- When clicking “Scan QR Code”, the mobile camera needs to be enabled and allowed.

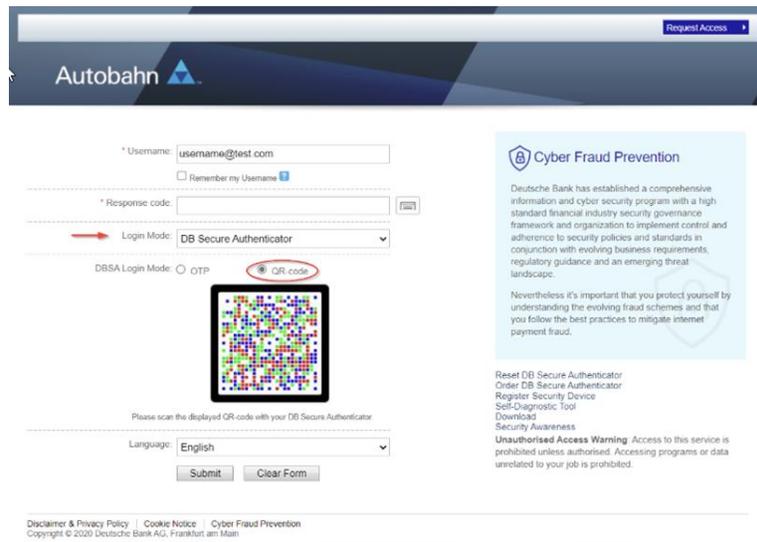


## 5.2 Logging in with DB Secure Authenticator (After Activation)

Instructions on how to log in using either the DB Secure Authenticator (DBSA) app or physical token, scanning the QR code or using the One Time Password (OTP) to log in.

### **Logging in using a QR Code**

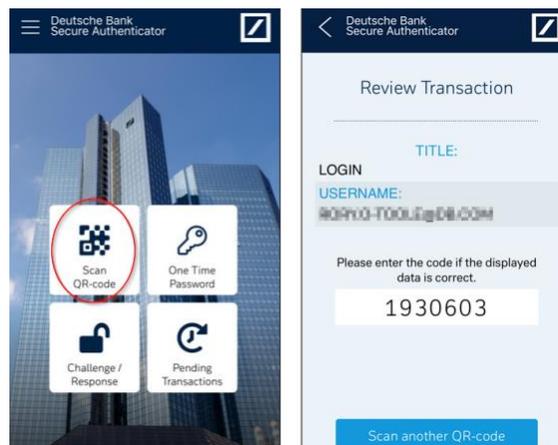
- When clicking “Scan QR Code”, the mobile camera needs to be enabled and allowed.
- Select the QR-CODE Option



The screenshot shows the Deutsche Bank login interface. At the top, there is a "Request Access" button. Below it, the "Autobahn" logo is visible. The login form includes fields for "Username" (pre-filled with "username@test.com") and "Response code". A "Remember my Username" checkbox is present. The "Login Mode" is set to "DB Secure Authenticator". Under "DBSA Login Mode", the "QR code" option is selected and circled in red. A QR code is displayed on a mobile device screen. Below the QR code, there is a "Language" dropdown menu set to "English" and "Submit" and "Clear Form" buttons. On the right side, there is a "Cyber Fraud Prevention" section with text about Deutsche Bank's security program and a list of links: "Reset DB Secure Authenticator", "Order DB Secure Authenticator", "Register Security Device", "Self-Diagnostic Tool", "Download Security Awareness". At the bottom, there is a disclaimer and copyright notice: "Disclaimer & Privacy Policy | Cookie Notice | Cyber Fraud Prevention Copyright © 2020 Deutsche Bank AG, Frankfurt am Main".

### **With the DB Secure Authenticator Mobile App**

- Launch the DB Secure Authenticator (DBSA) mobile app.
- Insert your six-digit PIN to open the app.
- Select “Scan QR-Code” option.
- Scan QR-Code displayed on the computer screen.
- Insert code generated by the app into Response Code field and press Submit.



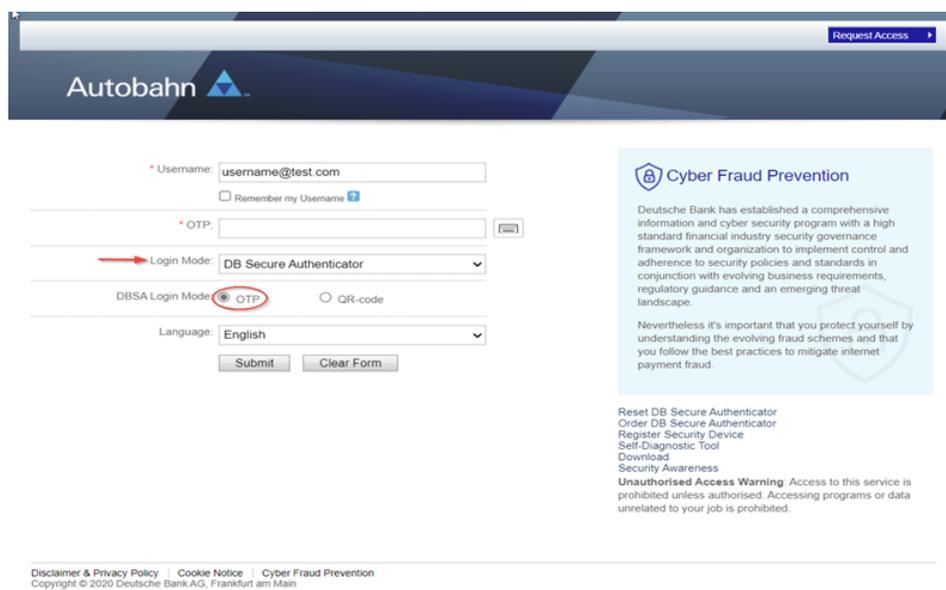
### With the DB Secure Authenticator Physical Token

- Switch on the physical token device by pressing the POWER button.
- Scan QR-Code displayed on the device logging in.
- Insert six-digit PIN.
- Insert the code generated by the device into Response Code field on device logging in.



### Logging in using an OTP (one-time password)

- Using a device, log into <https://autobahn.db.com/login>
- Insert your username and select login mode as DB SECURE AUTHENTICATOR.
- Select the OTP option.



Request Access

Autobahn

\* Username:   Remember my Username

\* OTP:

Login Mode:

DBSA Login Mode:  OTP  QR-code

Language:

**Cyber Fraud Prevention**

Deutsche Bank has established a comprehensive information and cyber security program with a high standard financial industry security governance framework and organization to implement control and adherence to security policies and standards in conjunction with evolving business requirements, regulatory guidance and an emerging threat landscape.

Nevertheless it's important that you protect yourself by understanding the evolving fraud schemes and that you follow the best practices to mitigate internet payment fraud.

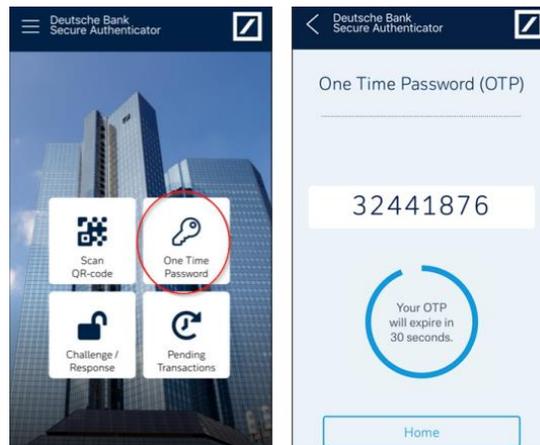
Reset DB Secure Authenticator  
Order DB Secure Authenticator  
Register Security Device  
Self-Diagnostic Tool  
Download  
Security Awareness

**Unauthorised Access Warning:** Access to this service is prohibited unless authorised. Accessing programs or data unrelated to your job is prohibited.

Disclaimer & Privacy Policy | Cookie Notice | Cyber Fraud Prevention  
Copyright © 2020 Deutsche Bank AG, Frankfurt am Main

### With the DB Secure Authenticator Mobile App

- Launch the DB Secure Authenticator (DBSA) mobile app.
- Insert your six-digit PIN to open the app.
- Select “One Time Password” option.
- Insert OTP into login screen and press submit.



### With the DB Secure Authenticator Physical Token

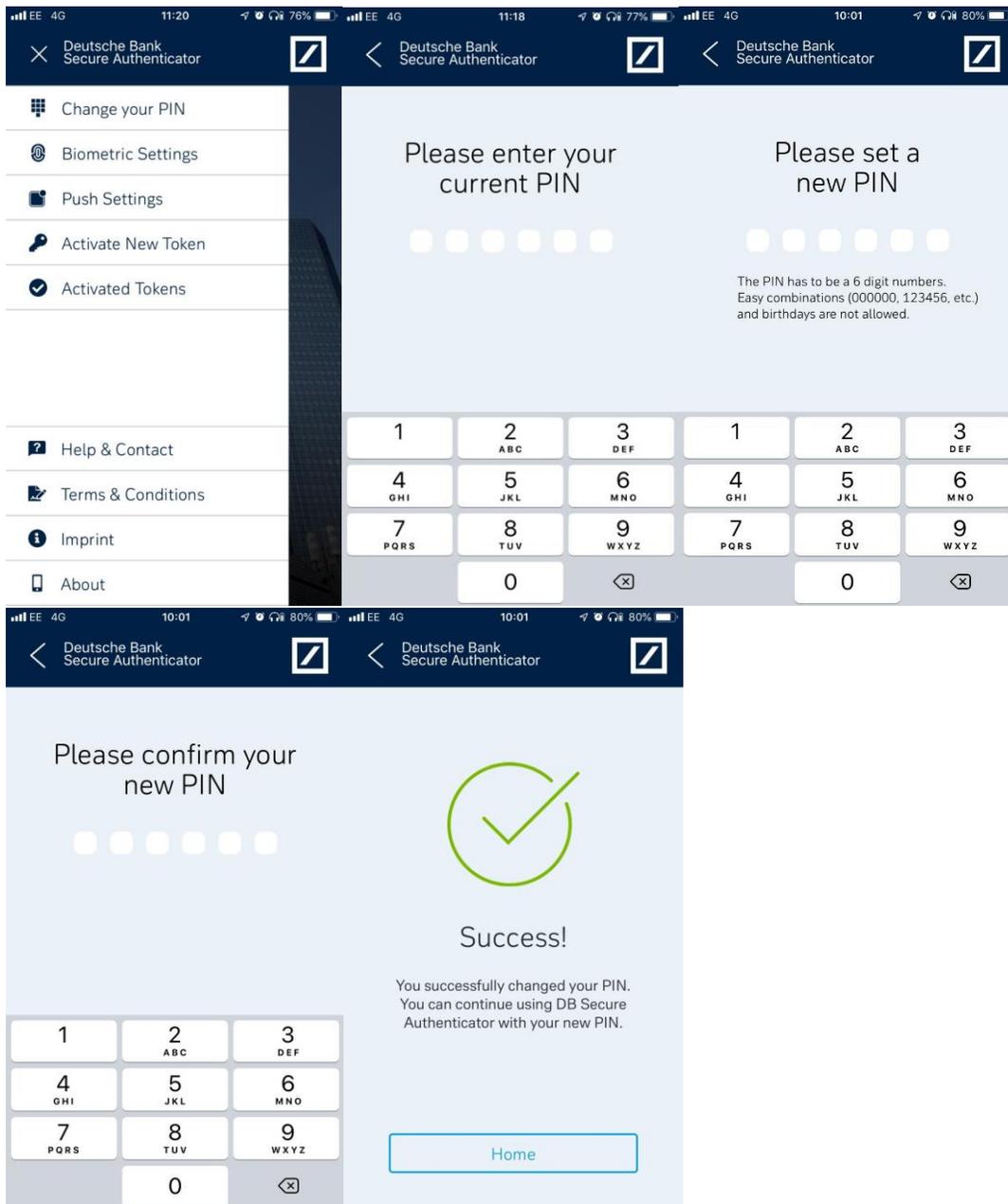
- Switch on the physical token device by pressing the POWER button.
- Insert six-digit PIN.
- Insert OTP into login screen and press submit.



## 6.0 DBSA Settings (For mobile application)

### 6.1 Change DBSA Login PIN – for mobile app

- Click “Change your PIN”.
- Enter your current PIN.
- Set a new desired PIN.
- Confirm the new desired PIN by re-entering it in.
- Success.



## 6.2 Activate multiple soft tokens.

- Log-in to [https://login.iss0.db.com/webss0/sso\\_multi\\_auth\\_flex\\_Logon.sso](https://login.iss0.db.com/webss0/sso_multi_auth_flex_Logon.sso) with DBSA as a login mode/

- Click on “Add New Device” to get to the activation screen

Name	Description
Autobahn Insight	Autobahn Insight
db-direct internet	db-direct internet
db-direct internet	Deutsche Bank's db-direct internet provides a single global platform for corporates and financial institutions to access cash management, FX, trade finance and domestic custody services.
db-direct internet	Deutsche Bank's db-direct internet provides a single global platform for corporates and financial institutions to access cash management, FX, trade finance and domestic custody services.
db-FSF	db-FSF
DBDI	db-direct Internet (dbdi) is the Internet based global electronic banking channel used by GTB business for providing cash, Trade and custody related functions.

Services | Help | Language Settings Internet Search

You are here: [Activation Code](#)

---

Welcome **Activation Code**

[Add New Device](#)

Logout

Please use your DB Secure Authenticator to scan the first activation QR code.

First activation QR code: 

First activation code:

Second activation code:

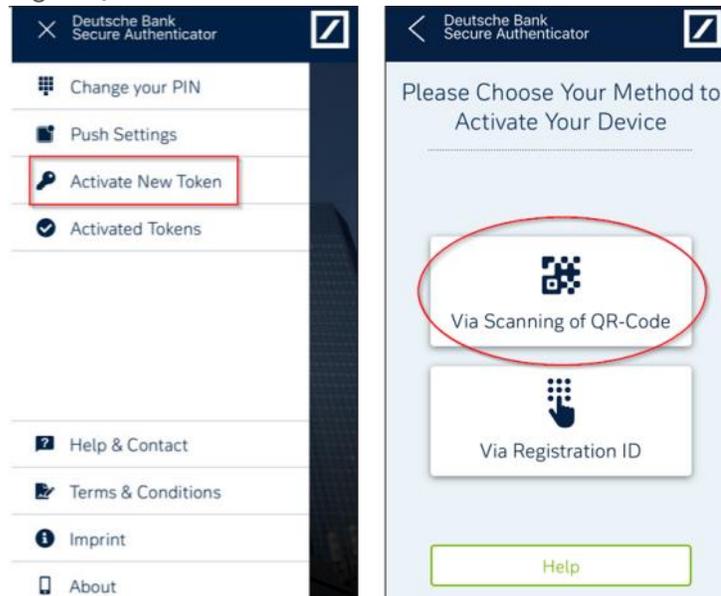
**Updates**

**Security Notification**

The media has reported on a security breach affecting encryption software "OpenSSL". We have updated your access certificate as a precautionary measure.

To this end, we kindly also ask you to change your Password for security reasons.

- On your DB Secure Authenticator Mobile App, select “Activate New Token”
- Press “Via Scanning of QR Code”

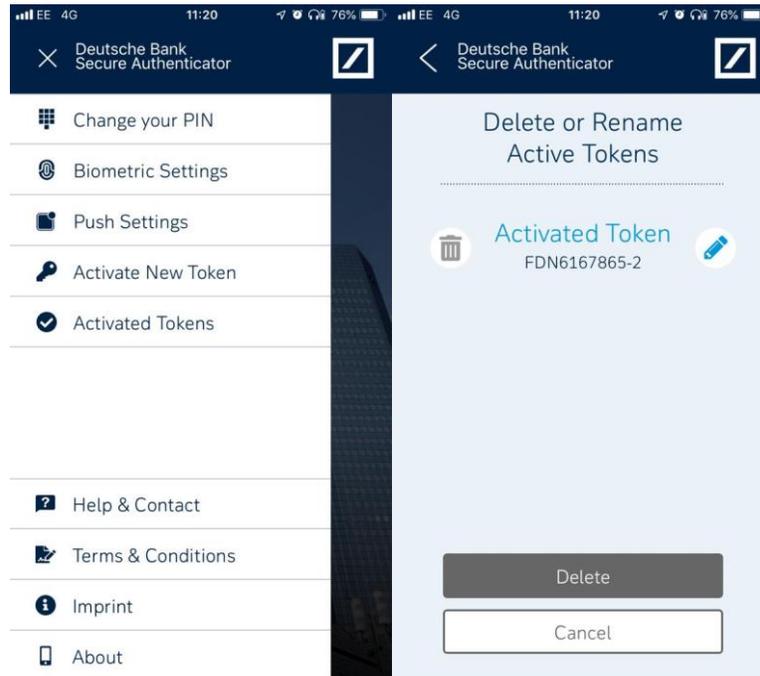


- Follow steps 3.6 from the earlier section onwards to activate the token.

### 6.3 Change Token ID name in case of multiple tokens (mobile app)

If you have more than one Token ID installed on a mobile device, it may be hard to identify the token ID based on the FDN number. Hence, you can add a name to easily recognise the token.

- Click on “Activated Tokens”
- Click on the pencil icon of the token to be updated
- Add a new name.



### 6.4 Delete an activated token.

- Select “Activated Tokens”
- Press the trash icon next to the token you would like to delete
- Press “Delete”

## 7.0 DBSA Settings (For hardware device)

DBSA hardware tokens are not available for DB China.

### 7.1 Enter Settings

- Press and hold POWER button for 5 seconds.
- Use left grey button to scroll across options.



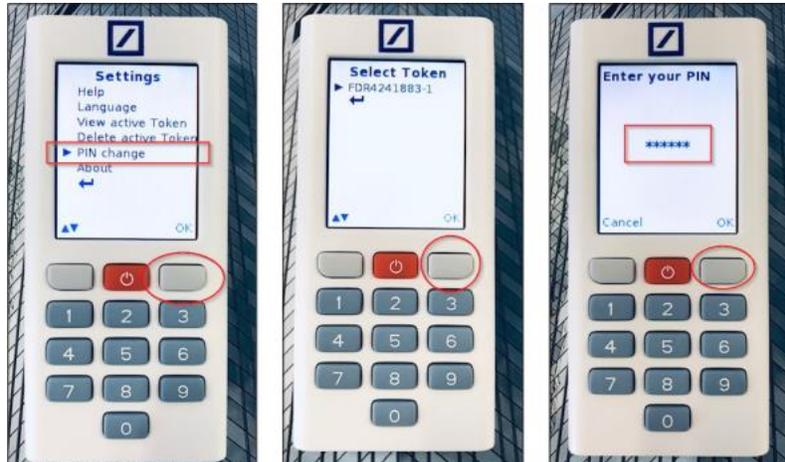
### 7.2 Select Language

- From the settings menu in 7.1, select the language option
- Press OK
- Scroll and select the desired language
- Confirm your selection.



### 7.3 Change Device PIN

- From the settings menu in 7.1. Select PIN change and press OK
- Select Token
- Enter PIN to confirm.



- Enter your new desired PIN.
- Confirm PIN.
- Press Continue.



## 7.4 Delete Active Token

- From the settings menu in 7.1. Select “Delete Active Token” and press OK.
- Select the token.
- Enter the device’s PIN.



- Confirm deletion.
- Acknowledge deletion.
- To activate a new token, follow steps 4.0 onwards.



## 8.0 Reset your DB Secure Authenticator

### 8.1. Go to Autobahn and click “Reset DB Secure Authenticator”

Deutsche Bank Authentication Gateway

Deutsche Bank Group

Services | Help | Language Settings

Internet Search

You are here: Services | Login

**Login**

System Requirements

**Reset DB Secure Authenticator**

Order DB Secure Authenticator

Change Password

Forgot Password?

Register Security Device

Self-Diagnostic Tool

Download

### Welcome to the Authentication Gateway (Web SSO) Login

Choose your Login Mode:

Password

\* Please enter your Email

Remember my Username

\* Please enter your Password

Fields marked with an asterisk (\*) must be completed.

Unauthorised Access Warning: Access to this service is prohibited unless authorised. Accessing programs or data unrelated to your job is prohibited.

Clear Form Submit

**Updates**

**Security Notification**

The media has reported on a security breach affecting encryption software "OpenSSL". We have updated your access certificate as a precautionary measure.

To this end, we kindly also ask you to change your Password for security reasons.

### 8.2. Provide your username to receive reset confirmation

Leave the window open

Services | Help | Language Settings

Internet Search

You are here: Services | Reset DB Secure Authenticator

**Login**

System Requirements

**Reset DB Secure Authenticator**

Order DB Secure Authenticator

Change Password

Forgot Password?

Register Security Device

Self-Diagnostic Tool

Download

### Reset DB Secure Authenticator

Enter user name to reset DB Secure Authenticator

Username:\*

Please note that if you have more than one DB Secure Authenticator active, you wont be able to login with any of the devices. All the devices have to be activated again.

Submit

**Updates**

**Security Notification**

The media has reported on a security breach affecting encryption software "OpenSSL". We have updated your access certificate as a precautionary measure.

To this end, we kindly also ask you to change your Password for security reasons.

---

**Login**

System Requirements

**Reset DB Secure Authenticator**

Order DB Secure Authenticator

Change Password

Forgot Password?

Register Security Device

Self-Diagnostic Tool

Download

### Reset DB Secure Authenticator

Your username is submitted successfully. Please check your registered email for next steps. In case your user profile is not eligible for pin self-reset option, you will not receive an email and we advise you to contact your known service desk.

OK

**Updates**

**Security Notification**

The media has reported on a security breach affecting encryption software "OpenSSL". We have updated your access certificate as a precautionary measure.

To this end, we kindly also ask you to change your Password for security reasons.

### 8.3. Confirm the reset of the DB Secure Authenticator

Click the button “Yes, I confirm” to confirm the rest of the token.

Confirmation to reset your DB Secure Authenticator

db-direct.alerts@db.com  
To: Harish Bisht  
Expires: 11/29/2027  
Fri 11/29/2024 12:25 PM

Retention Policy Email Retention Policy (3 years)  
If there are problems with how this message is displayed, click here to view it in a web browser.



Dear dbsa\_0069 user\_0069,

We have received a request to reset your DB Secure Authenticator which was being used for username [dbsa\\_0069@test.com](#). Was this request sent by you? If so please confirm by clicking the button below so that we can proceed further.

Please note that if you have more than one DB Secure Authenticator active; you won't be able to login with any of the devices. All the devices have to be activated again.

[Yes, I confirm](#)

Deutsche Bank Authentication Gateway Deutsche Bank Group

Services Help Language Settings Internet Search

You are here: Services | [Reset DB Secure Authenticator](#)

## Reset DB Secure Authenticator

Login

System Requirements

Reset DB Secure Authenticator

Order DB Secure Authenticator You're all set!

Change Password

Forgot Password? You just confirmed it was you. Further instructions have been sent to your email account.

Register Security Device

Self-Diagnostic Tool

Download

Updates

Security Notification

The media has reported on a security breach affecting encryption software "OpenSSL". We have updated your access certificate as a precautionary measure.

To this end, we kindly also ask you to change your Password for security reasons.

### 8.4. Deactivate your actual tokens (software or hardware)

You would have received a new welcome email providing instructions on how to reset your DB Secure Authenticator.

To reset the DB Secure Authenticator Mobile App, please uninstall and re-download the app.

If you are using a DB Secure Authenticator hardware token, please enter an incorrect PIN five times to reset the token.

### 8.5. Re-activate your actual tokens (software or hardware)

To reactivate your token, please follow the steps displayed in the welcome email, and the steps captured in section 3 and section 4 of this user guide.

This user guide is for information purposes only and is designed to serve as a general overview regarding the services of Deutsche Bank AG, any of its branches and affiliates. The general description in this user guide relates to services offered by Corporate Bank of Deutsche Bank AG, any of its branches and affiliates to customers as of April 2025, which may be subject to change in the future. This user guide and the general description of the services are in their nature only illustrative, do neither explicitly nor implicitly make an offer and therefore do not contain or cannot result in any contractual or non-contractual obligation or liability of Deutsche Bank AG, any of its branches or affiliates.

Deutsche Bank AG is authorised and regulated by the European Central Bank and the German Federal Financial Supervisory Authority (BaFin). With respect to activities undertaken in the UK, Deutsche Bank is authorised by the Prudential Regulation Authority. It is subject to regulation by the Financial Conduct Authority and limited regulation by the Prudential Regulation Authority. Details about the extent of Deutsche Bank AG's authorisation and regulation by the Prudential Regulation Authority are available from Deutsche Bank AG on request.

Copyright© April 2025 Deutsche Bank AG.

All rights reserved.