

Deutsche Bank Secure Authenticator

Helpdesk User Guide – DBSA PIN Reset


Document Version: 1.0

1. Soft token PIN Reset


Step 1: Go on WebSSO/Autobahn/Toolbar and click on “Reset DB Secure Authenticator”

Deutsche Bank
Authentication Gateway


Deutsche Bank Group



Request Access ▶

Autobahn 

* Username:

☐ Remember my Email 

* OTP:

Login Mode:

DB Secure Authenticator ▼

DBSA Login Mode: ☒ OTP ☐ QR-code

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

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

Step 2: Insert the Username and click on “Submit”



Reset DB Secure Authenticator

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.

* Username:

[Back to login](#)

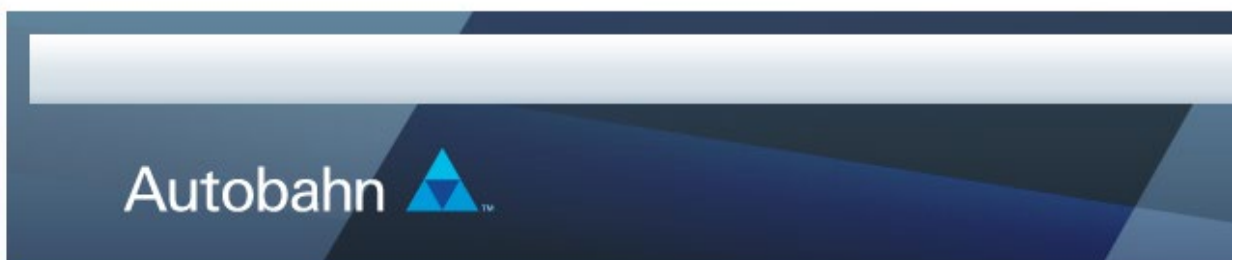
Cyber Fraud Prevention

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](#)
[Forgot Password?](#)
[Register Security Device](#)
[Self Diagnostic Tool](#)

Step 3: Press "OK" and you will now receive an email



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.

Step 4: Open the email and press “Yes, I confirm”

Dear dbsa 12051,

We have received a request to reset your DB Secure Authenticator which was being used for username dbsa12051@test.com. Was this request sent by you? If so please confirm by clicking the button below so that we can proceed further.

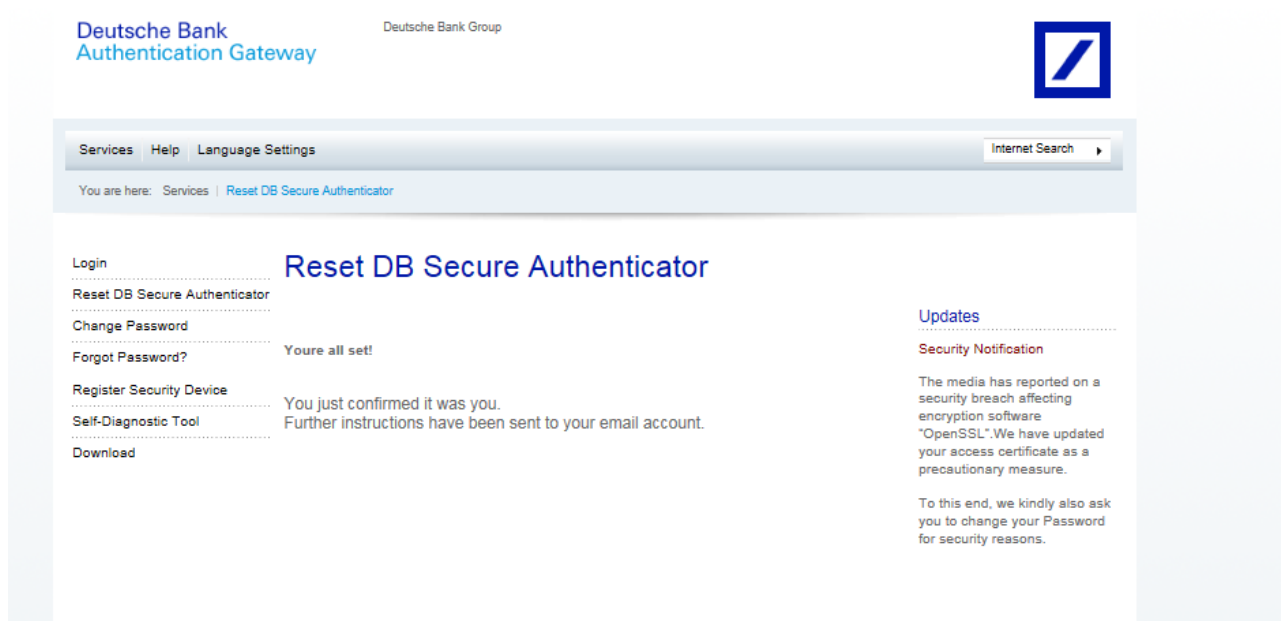
Please note that if you have more than one DB Secure Authenticator active; you won't be able to login with any of the devices. All the devices have to be activated again.

Yes, I confirm

Please contact service desk if you did not request for pin reset.

Kind Regards,

Autobahn App Market Support

Step 5: WebSSO will open automatically and you will receive a new email again**Step 6: Open the email and follow the steps in the email**

Message Password.pdf (2 KB)



Dear dbsa 12051,

You have requested for your DB Secure Authenticator to be reset.
Kindly complete the following steps to reset DB Secure Authenticator.

DB Secure Authenticator Soft Token users please follow below steps:

1. Delete the DB Secure Authenticator app from your mobile device.
2. Download DB Secure Authenticator app on your mobile.



3. A PDF file containing the password is attached; in this email.
4. For security reasons, the necessary code to open the attached PDF file has been sent to anna.sobuta@db.com
5. In order to get the code please call the email recipient mentioned in step 4 which may be your usual service desk or a colleague in your organization.
6. Open the PDF file using the code.
7. Open URL <https://autobahn.db.com/login>
8. On the login page click on "Register Security Device" link and select Password from Login Mode dropdown.
9. Use the Password contained within the pdf to log in.
10. After login; you will be asked to activate DB Secure Authenticator.
11. Please follow the online instructions to complete the Activation flow.

The passphrase to open PDF must be provided to the customer in a secure manner and this secure manner must exclude sending to the customers email account. **Why:** this is to ensure two distinct channels are employed to fulfil the 2factor security standard limiting the risk of identity theft.

Step 7: To activate account follow standard procedure, which can be found in link below:

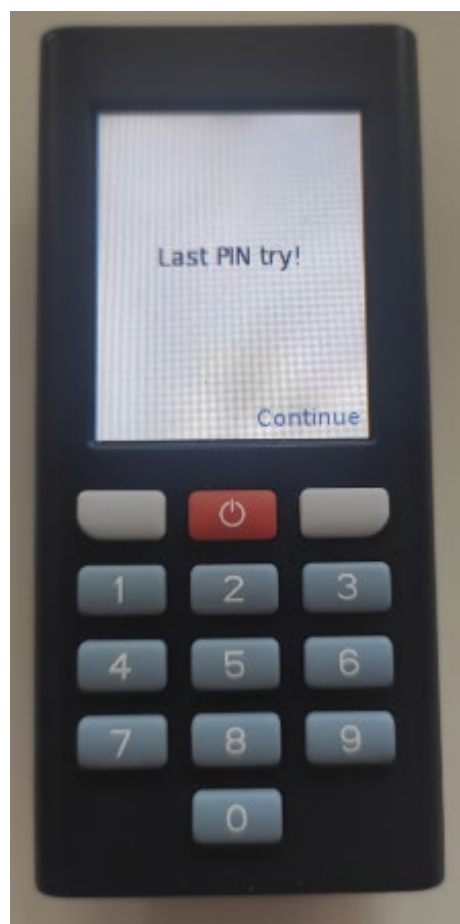
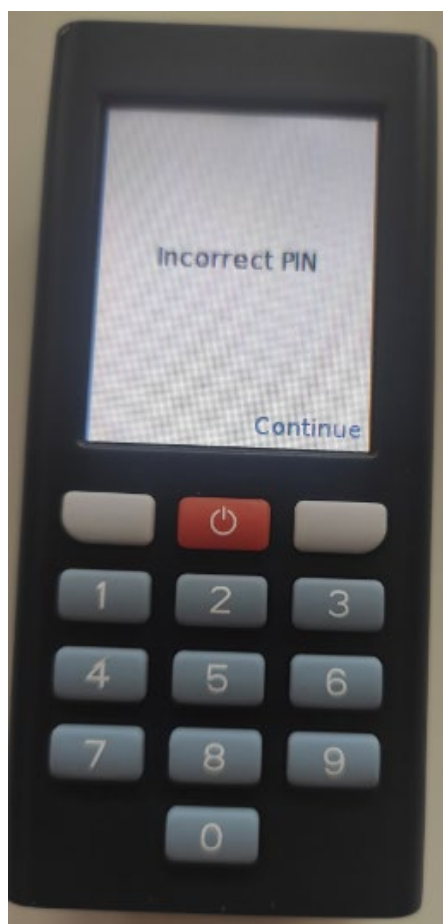
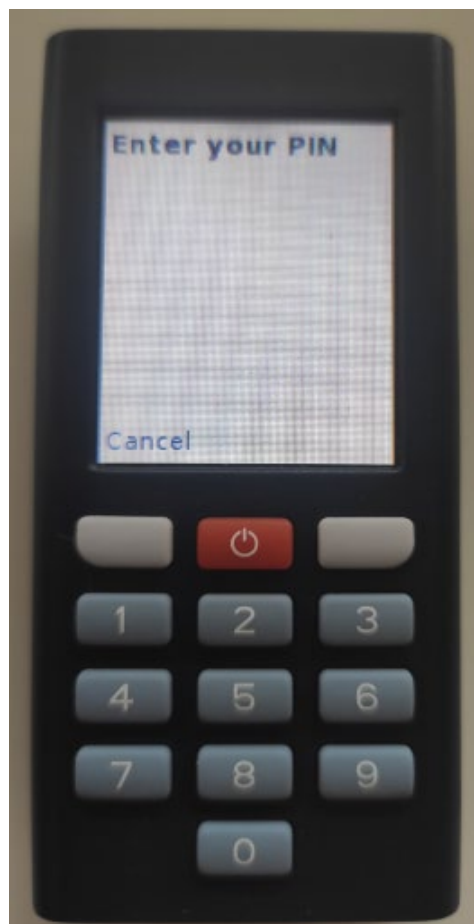
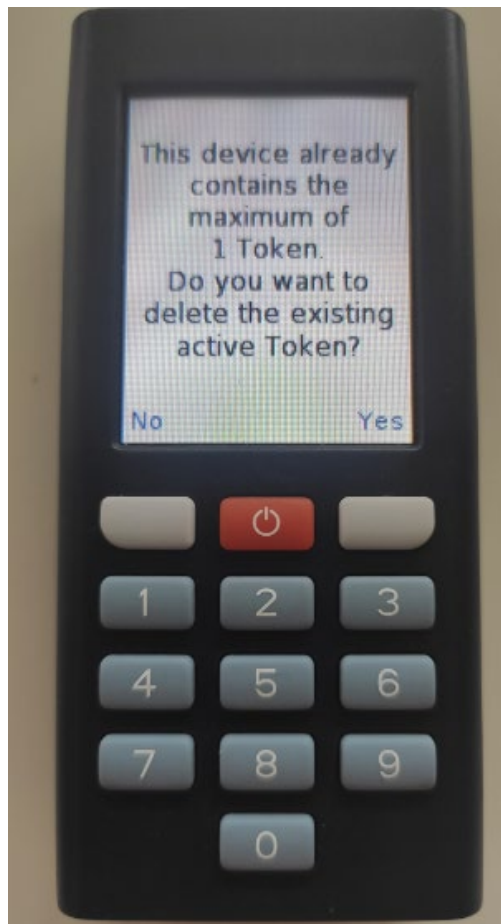
<https://autobahn.db.com/autobahn/guides/index.html>

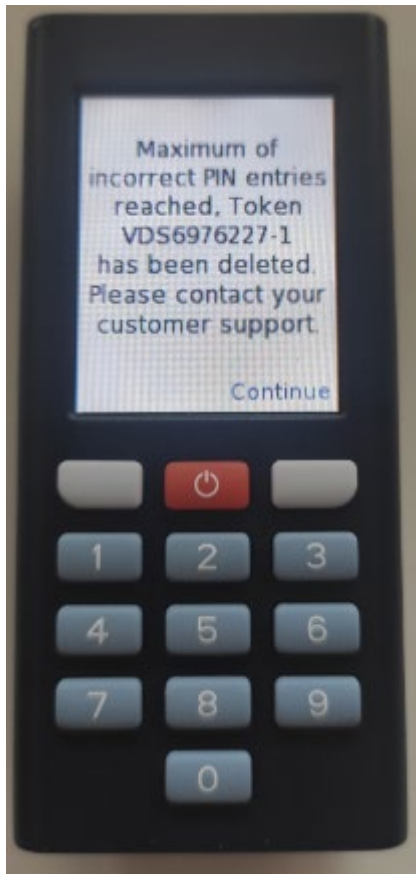
Login Experience → DB Secure Authenticator → Mobile App Activation (starting from Step 5)

2. Hard token PIN Reset -Not ready to be offered by DB China

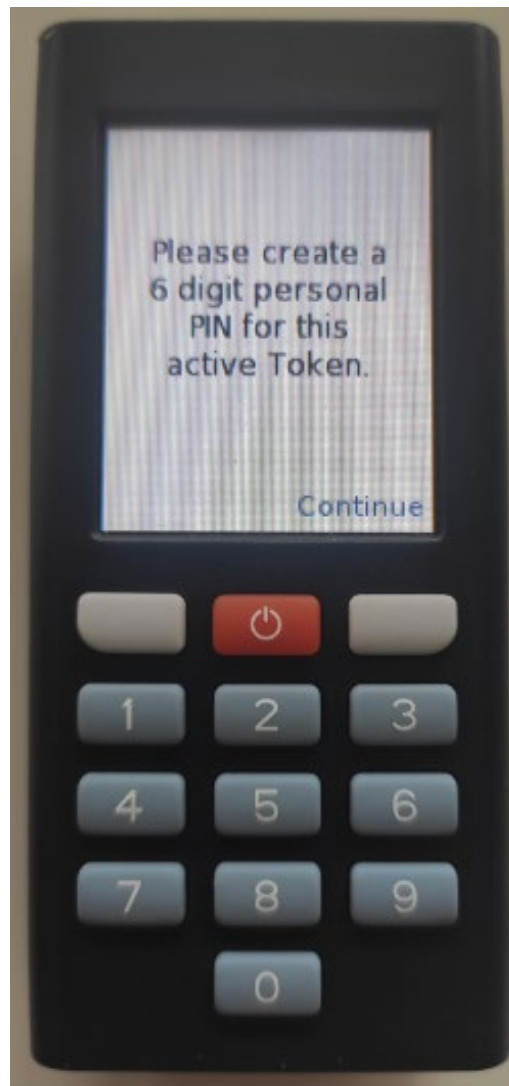
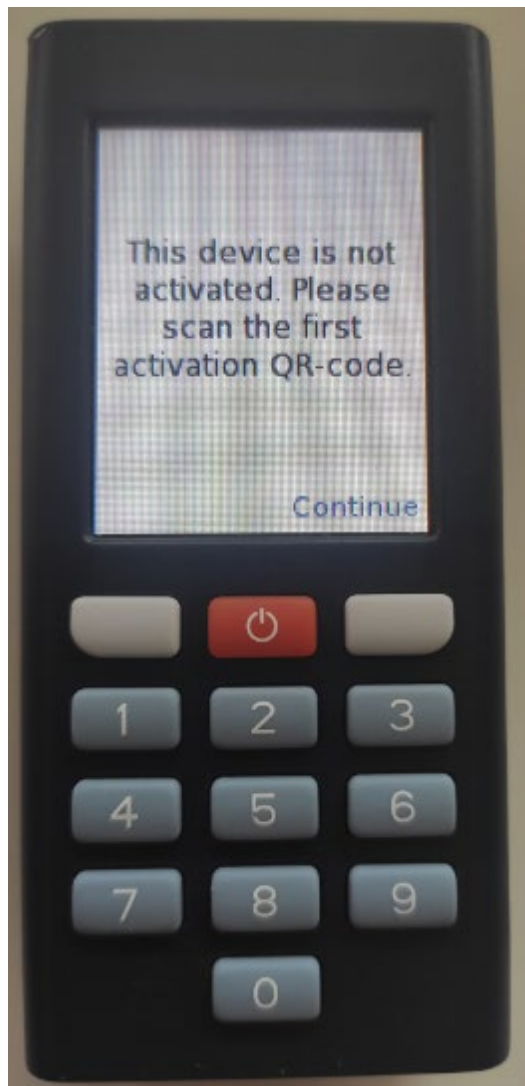
Step 1: In order to reset Password for Hard token Device please follow steps 1-6 from section above Soft Token PIN Reset.

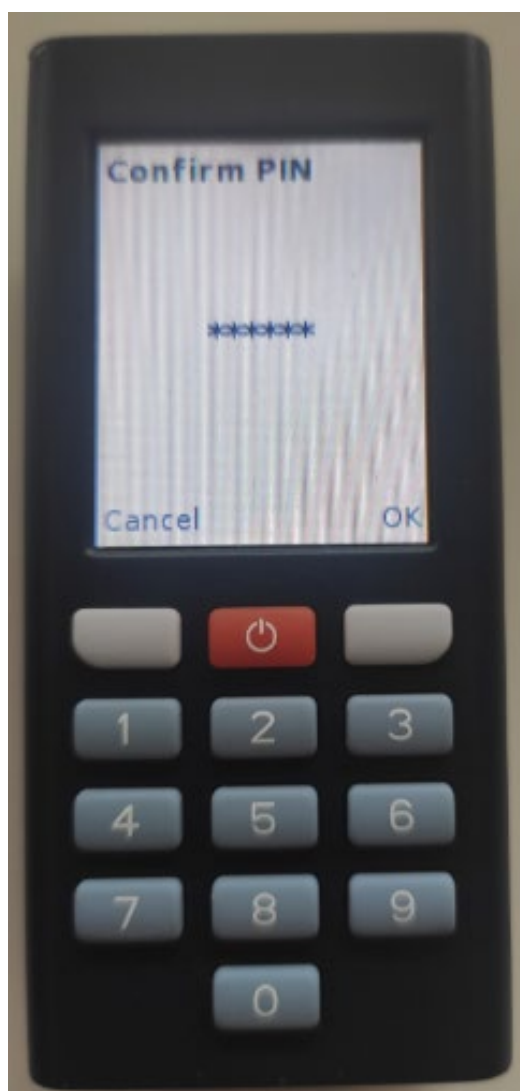
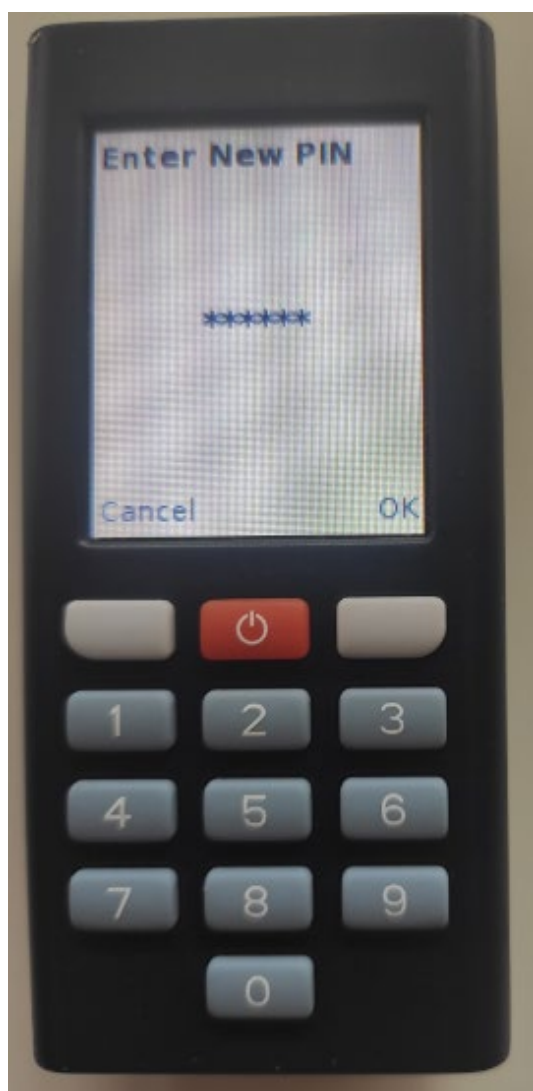
Step 2: Before the account can be activated Hard Token device need to be reset by entering incorrect PIN 3 times

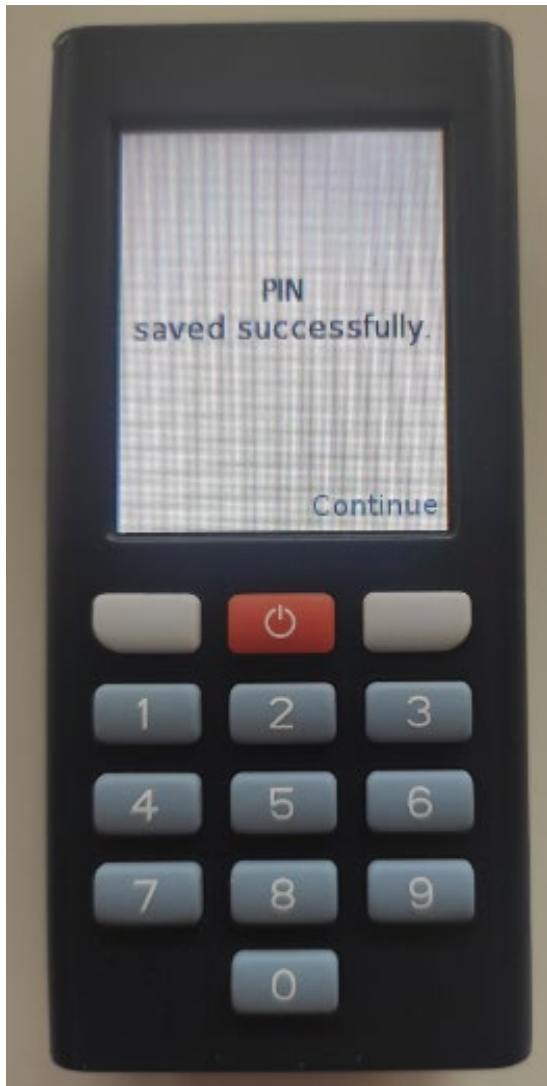




Step 3: After the old token is deleted, new PIN can be setup.







Step 4. Once new PIN is setup activation process can be completed following steps from procedure available under link below:

<https://autobahn.db.com/autobahn/guides/index.html>

Login Experience -> DB Secure Authenticator -> Hardware Token Activation (starting from step 3).