

# Deutsche Bank introduces DB Secure Authenticator

Due to new regulations such as General Data Protection Regulation (GDPR) and Payment Service Directive 2 (PSD2), Deutsche Bank will be introducing DB Secure Authenticator to ensure it is strengthening the security around clients' data online.

## What is DB Secure Authenticator?

DB Secure Authenticator is a new app available on iOS and Android which allows users of Global Transaction Banking online systems (e.g. the Autobahn App Market) to perform secure log-in and authorising transactions.

Using DB Secure Authenticator, users can key in their username on the usual [autobahn.db.com/login](https://autobahn.db.com/login) website and complete the log-in action with a One Time Password (OTP) which is generated on their smartphone. Generating the OTP requires a PIN code and as a result the log-in is secured by the 2-Factor Authentication standard, the PIN code being a knowledge factor, and the ownership of the registered smartphone app being a possession factor.

To authorise a transaction, the DB Secure Authenticator makes use of the smartphone's built in camera to scan the transaction details displayed online as cryptographic QR code. The app then displays the transaction details on the phone as well as a respective OTP to sign the specific transaction. A PIN code is needed before starting this process, ensuring the 2-Factor Authentication standard is met.

## Why is Deutsche Bank introducing DB Secure Authenticator?

Global regulations and in particular PSD2 within the EU seeks to strengthen the protection of sensitive payment data. PSD2 seeks to upgrade security at the point of log-in to online banking apps and at the point that transactions are authorised.

Deutsche Bank will also upgrade security whenever user changes that relate to the ability to create or alter payments are submitted online.

In any one of these scenarios (log-in, transaction authorisation, user detail changes), users will in future need to authenticate their actions using 2 of the following factors:

- Knowledge; something the user knows (such as a PIN code)
- Possession: something the user has (such as a security token)
- Inherence: related to who the user is (e.g. biometric data, fingerprint etc.)



When a payment is authorised, details of the payment must be included in the authorisation activity to link the payment to the specific authorisation act. DB Secure Authenticator allows to fulfil this regulation in a smooth way by scanning QR codes as described earlier.

[What if I do not want to use the DB Secure Authenticator? Or am not allowed to use DB Secure Authenticator?](#)

Deutsche Bank will not enforce soft tokens but allow users to choose between the soft and hardware version. For users who prefer not to use a smartphone or are not allowed to use a smartphone by their corporate policy for log-in or authorisation, Deutsche Bank can provide a small, hardware device that has the same DB Secure Authenticator capability.

[How can I upgrade to the new solution?](#)

After you have logged into the AutoBahn app you will be alerted that you can upgrade to the new DB Secure Authenticator.

Users who currently log-in only using a password will be alerted first, but in time all other users with outdated security devices / tokens will be asked to upgrade. Users will be given instructions how to download and register the new app. Existing log-in credentials as well as a valid email address will be enough to securely registering the app.

Users will be given the choice to order a hardware token if they cannot make use of the mobile app offering. Please note this choice is offered online to the individual user, rather than at the company level.

If the client has a preference for hardware devices for their users they will need to communicate that internally within their organisation ensuring end users make the right choice.

A valid postal delivery address is required for users opting for the hardware option.

[What are the technical requirements for the soft token?](#)

	iOS	Android
Minimum Version of Operating system	8.0	4.0.3
Size of application once installed	25 Megabyte	17 Megabyte

- If you update your phone to the latest operating system, the app will continue to work
- The app will need to have access to a camera
- After you have downloaded and installed the app, you will not need internet access to use the app
- Deutsche Bank advise users against using app on jailbroken/rooted devices
- There are no requirements on the size of the screen for the app

What are the differences between a software and hardware token?

Below outlines the differences between a Soft Token and a Hardware Token.

	Soft Token	Hardware Token
Overview	A Soft Token is an app installed on a user's private or corporate smart phone and is used to log-in or authorize transactions	A Hardware Token is a physical device that the user needs to carry around in order to log-in or authorize transactions
Device	No Hardware required, users only need a smartphone – please refer to the technical requirements	Hardware device with camera Technical name: DP770R Size: 90.22 mm (L), 42 mm (W), 9-16.88 mm (H) Weight: 32 gram
Updates	Easily allows Deutsche Bank to introduce new features to improve the user experience such as biometrics to replace the knowledge factor as well as “push” authentication. Updates to the technology can be easily made; ensuring that security standards can always be at the highest level	New features and updates cannot be deployed therefore a replacement device may be required if updates are mandatory
Battery life	No battery expiry	When the battery expires the user can load 2 new AAA batteries.
Ownership	If a user terminates their role the soft token can be remotely disabled	If a user terminates their role the Hardware device can be passed on to other users – after clearing the previous registration

Contacts and support (Autobahn, App Market)

Europe: + 44 20 7547 3030

Americas: +1 212 250 8651

Asia: +65 6423 5660

Email: [autobahn@db.com](mailto:autobahn@db.com)

This document 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 document relates to services offered by Global Transaction Banking of Deutsche Bank AG, any of its branches and affiliates to customers as of June 2018, which may be subject to change in the future. This document 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.

This communication has been approved and/or communicated by Deutsche Bank Group. Products or services referenced in this communication are provided by Deutsche Bank AG or by its subsidiaries and/or affiliates in accordance with appropriate local legislation and regulation. For more information: [www.db.com](http://www.db.com). Copyright © July 2018 Deutsche Bank AG. All rights reserved.

Deutsche Bank AG is authorised under German Banking Law (competent authorities: European Central Bank and German Federal Financial Supervisory Authority (BaFin) and, in the United Kingdom, by the Prudential Regulation Authority. It is subject to supervision by the European Central Bank and the BaFin, and to limited supervision in the United Kingdom by the Prudential Regulation Authority and the Financial Conduct Authority. Details about the extent of our authorisation and supervision by these authorities are available on request.

Copyright© July 2018 Deutsche Bank AG.

All rights reserved.