ABFX on Mobile

A security FAQ for clients

Autobahn 

Contents

Authentication and Access

Mobile Device Requirements

Rooted Devices

The Autobahn application will not start on rooted or jail-broken devices.

Device protection with PIN code or biometric

The Autobahn application will not work unless a device is protected with either PIN code or biometric authentication (fingerprint or face recognition).

Login

User authentication

The Autobahn application supports one factor authentication (login/password) and two factor authentication (2FA).

For 2FA first factor is the possession of the mobile device and the second factor is the knowledge of the PIN code. The DB Secure Authenticator application is used for 2FA.

If 2FA is enabled for particular user it becomes the only login option, no login with login/password will then be possible for that user.

Users credentials transmitting and storing

Login credentials (password or token) are transmitted over TLS protected channels.

The application does not store user credentials on the mobile device or on the backend.

User Session

Are parallel sessions allowed from different devices?

Parallel sessions are allowed for Desktop and Mobile; for two Mobile devices the latest session will forcibly logout the oldest.

User session lifetime and timeout

The Maximum lifetime for user session is 5 days (business week - Monday to Friday). The session is automatically logged off at Friday end-of-day.

When automatic logoff happens, a user needs to login again.

If the Autobahn application is not used for 30 mins it is locked automatically, and should be unlocked by the user to continue using it.

Session credentials (tokens, API keys) protection

The Autobahn application stores ***session*** credentials in secure storage on the mobile device through an iOS or Android API. This storage is accessible only by the Autobahn Application.
Applications store session credentials as a secure cookie in the embedded browser.

Privacy and Data Protection

Data on Device

How the data stored on device is protected?

All sensitive data is stored in secure storage through an iOS or Android API. This storage is accessible only by the Autobahn Application.
No sensitive data (application metadata: display name, user layout) is stored in the application folder.

Does the application store secret passwords or keys on the device?

No.

Could sensitive information leak from application logs?

There is no sensitive information stored in plaintext in application logs.

Network

Data transmission between Mobile application and Deutsche Bank

All data is transmitted over TLS protected channels. AES128 and AES256 are used for data encryption.

We use only TLSv1.2 and strong ciphers with the PFS (perfect forward secrecy) property. The supported ciphers are regularly revised against Cryptography community recommendations and local DB policies; weak ciphers are excluded.

Deutsche Bank endpoints identity verification

Deutsche Bank endpoints identity is protected by the Digicert certificate authority. Server certificates are EV (extended validation).

Shared Services

Phone services required for running the application

The application needs optional permission for push notifications and mandatory permission for Geo-location services. On an Android device access to the shared drive is required to be able to send logs via email for troubleshooting purposes (in case in-app send-logs fails).

Device Lost/Theft Protection

Data Leakage

Could application data be erased in case the device is lost or stolen?

All the application data could be erased using standard theft protection features provided by Apple/Google.

Access Leakage

Could an unauthorized person gain access to the application?

The application is protected by authentication and there is no way to circumvent it.
To minimize the risks of unauthorized access please use strong passwords and do not share your credentials. Always lock your device when you are not using it.

Could access to the application be revoked in case the device is lost or stolen?

Yes. Please contact your sales representative or IT support via autobahn.fx@db.com.

Accidental Actions Protection (fat finger, pocket dial)

1. Accidental trading protection – a user has to unlock trading by tapping the unlock icon once. Trading is disabled again in 15 seconds
2. Accidental order cancel protection: users have to confirm when requesting order cancellation
3. Order placement cannot happen accidentally as a user has to enter order details before order placement

Contact:

For technical assistance, please contact the Autobahn App Market and Toolbar Support team:

Email: autobahn.info@db.com

https://autobahn.db.com/microSite/html/contacts.html

Autobahn