GAZPROMBANK
(SWITZERLAND) LTD

E-BANKING USER GUIDE

Version November 2021

GAZPROMBANK (SWITZERLAND) LTD.

Table of contents **Page**

1 FIRST LOGIN

Before the first login, please make sure that you have received from the Bank the following: Letter with the **Contract Number**, **or PIN and the initial Password.**

Depending on your preference, you have received a **physical Token**, or an **activation letter for activating the mobile app GPBS Authenticator** available for Android- or iOS-devices.

Please refer to the respective chapters below for the physical Token setup (ref 1.1) and GPBS Authenticator (ref 1.2)

1.1 Changing the PIN on your Token

Each Token is protected by the initial PIN code assigned during token initialization. In accordance with E-Banking Terms and Conditions, after receiving a Token from the Bank it is necessary to change the PIN code immediately by completing the following steps:

- Turn on your Token by pressing the green “power” button;
- Enter the PIN code you received from the Bank. The Token displays a ‘*’ character for each number you enter;
- Press the green “power” button;
- Press the “down arrow” button until you see “CHANGE PIN”;
- Press the green “power” button to confirm;
- When “NEW PIN” appears, enter a new, four-digit PIN;
- Press the green “power” button to confirm;
- When “CONFIRM” appears, re-enter your new PIN;
- Press the green “power” button to confirm;
- The message “COMPLETE” appears, confirming that your new PIN has been set successfully.

From now on, use your new PIN with the Token when you want to log in to E-Banking.

1.2 Installation of the GPBS Authenticator & Initial Login

If you received the initial activation letter with the respective pictogram, during your first login you can setup your mobile device for second factor authentication.. In order to activate this method, please follow the below steps.

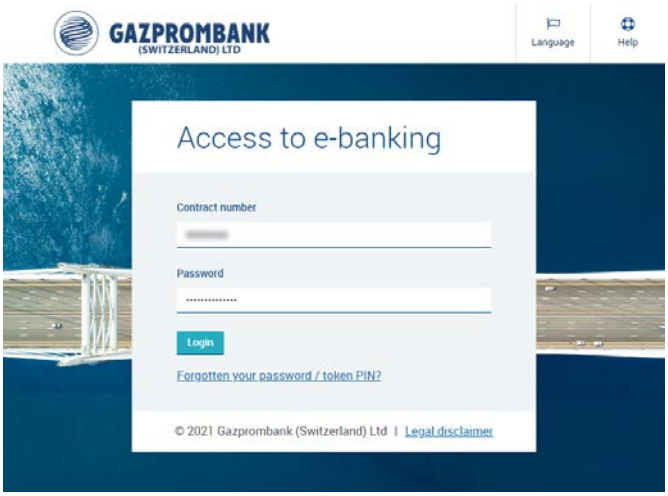
Download the App, searching for "GPBS Authenticator" in the App-Stores or download them via the following links:

Available on the App Store GET IT ON Google Play

1.3 Login

In order to login into the E-Banking system, please use the link https://pay.gazprombank.ch.

Enter your Contract number and Password:



Depending on your choice regarding authentication method, you have to proceed with App or Token.

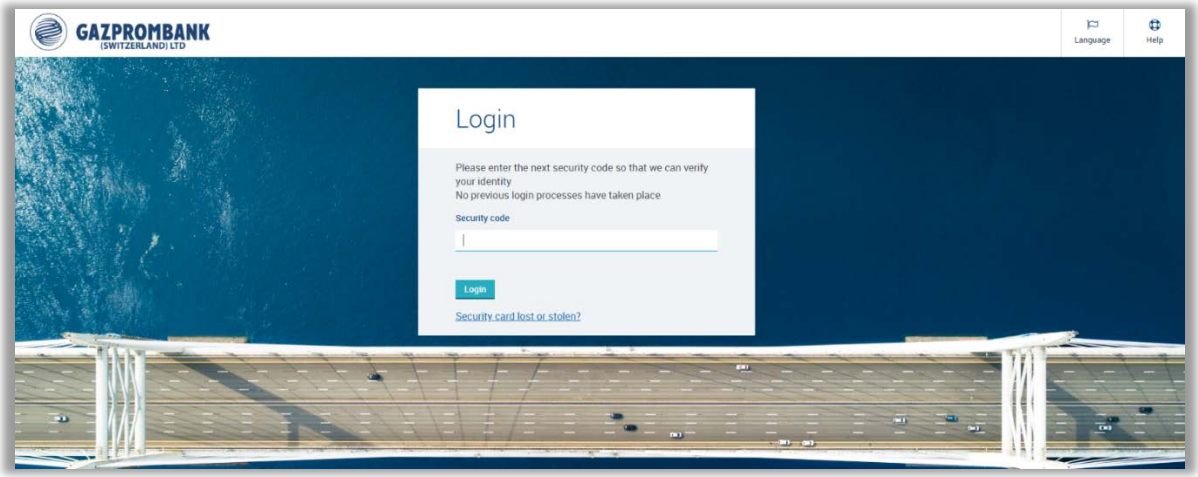
1.3.1 Authentication via App - Scan the initial activation code received

- Open the app, scan the image on your letter and enter the numerical activation code in the field marked “Code”, click “Verify”.
- On the screen, you have to scan the next image and enter the shown code to finalize the setup of your device. Optionally, you can enter also a name for your device. After you entered that information, you are redirected to the main page of the E-Banking.

1.3.2 Authentication via Token - Generate a security code with your Token:

- Turn on your Token by pressing the green “power” button.
- Type in your PIN code. The Token displays a ‘*’ character for each number you enter.
- A numerical password appears on the Token screen.

Enter the numerical password in the field marked “Password”, click “Next” and then “Start E-Banking”.



2 MOBILE BANKING APP

A mobile app "GPBS Mobile Banking" has been introduced for Android and iOS devices. The app can be used right away with an existing authentication setup of E-Banking Users. The main functionalities of the mobile app include Wealth Dashboard, which displays list of current accounts and balances, quick access to payments and their status. Portfolio details allow portfolio overview, performance and analysis. Further functionalities such as Payments and Trading will be released in 2022.

2.1 Activation

To use the mobile app with your contract, you have to activate it in the settings accessible in the e-banking interface.

- Select "Account & profile" → General
- Activate on the option "Enable mobile banking" and confirm by clicking "Save".

2.2 Login

To access the mobile app you have to login with your contract number and your password.

You will be able to access the app with the same authentication method as you access the e-banking in the browser.

2.3 Capabilities

The current functionality is available in your mobile app:

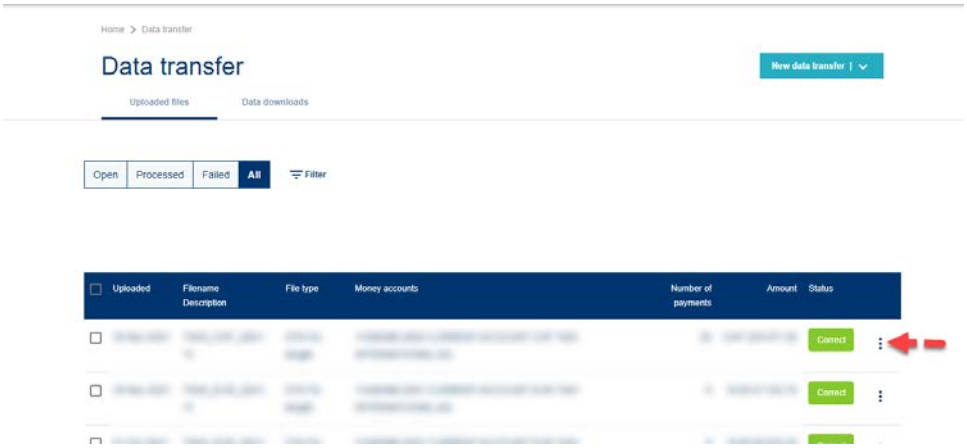
- Portfolio View
- Account Overview & Analysis
- Communication capabilities to interact with the Bank
- Document safe

3 PAYMENTS – SPECIAL CASES

3.1 Salary payments – DTA file

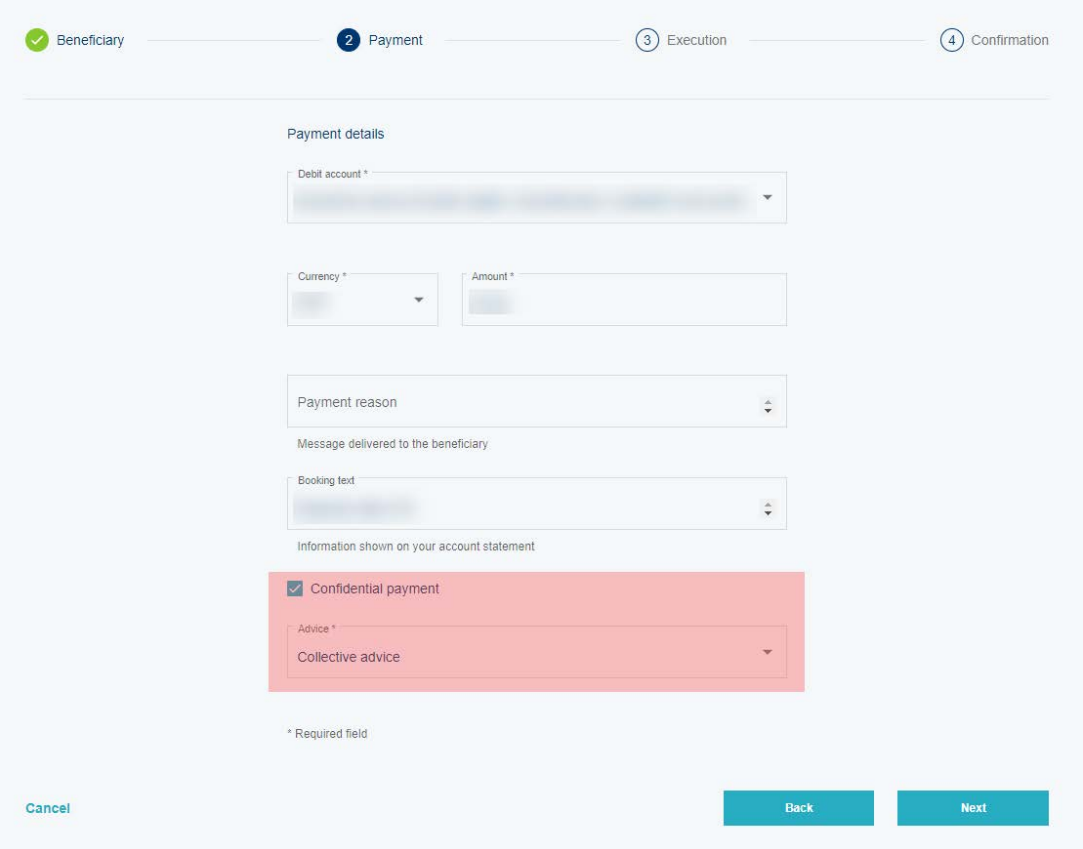
To ensure the confidentiality of salary payments we recommend uploading them as a single file in DTA format using the menu item **Data Transfer ➞ New.** In the field "Debit note" option "Collective confirmation document" should be selected. This option will allow to group all payments in one record (mass payment) in the account statement. All payments should be marked as "Confidential payments" so that users without respective rights will not be able to see details of such payments.

After uploading a file, User should send it for processing by clicking the three dots as shown below and select "Proceed".



3.2 Salary payments as separate orders

If salary payments are inputted manually, it is necessary to select options "Collective advice" and "Confidential payments" for each individual payment.



IMPORTANT: If there is only one salary payment, it is necessary to fill in the field "Booking text". The information entered in the field "Booking text" will replace the Beneficiary name in the Account Statements, so that users without access to Confidential Payments will be able to see "Booking text", but not the name of the Beneficiary.

4 SECURITY INFORMATION

Up-to-date information protection technologies used in the E-Banking system enable to secure the information exchange between the Client and the Bank. However, the computers and other electronic devices of the Client being part of the E-Banking system may face potential risks of the Internet. Therefore, the Bank strongly recommends its Clients to follow the security rules:

4.1 PIN, Token, Password and Contract number

- Change the PIN on your Token immediately after receiving the Token from the Bank.
- Keep your Token in a safe place.
- If your Token, Contract number, Password and/or PIN have been compromised, stolen or lost, please contact your Relationship Manger immediately.
- Please ensure that your Password and PIN code are difficult to guess. Avoid using dates of birth, popular combinations such as "1234," "1111," "0000" etc. Do not use a password that you have previously used elsewhere on your computer or in the Internet.
- The best way is to memorize your Password and PIN code. However, if you do need to write them down, keep them in a safe place and NOT together with your Token. Do not disclose your Password or PIN to anyone.

4.2 Computer security

- Use anti-virus and firewall software on your computer. Configure the security software to update virus lists automatically and regularly in order to minimize risk.
- Keep your operating system, browser, anti-virus, firewall and other software updated.
- Do not install software from untrustworthy sources. Always check the origin of files to be downloaded from the Internet.
- Turn off your computer completely when you are finished using it – do not leave it in sleep mode.
- Configure your devices to prevent unauthorized users from accessing your network remotely.
- Close all other Internet applications before connecting to E-banking system.
- Do not leave your computer unattended when the E-Banking session is active.
- Log-off after you finish using E-banking system.

4.3 Mobile Phone security

- No Rooted device (Jailbreak)
- Do not give other users access to your biometrics (face- or touch-ID)
- Keep your operating system, apps and other software updated

4.4 Protection against fraudulent e-mails

- Do not send confidential information by e-mail.
- Be wary of suspicious e-mails. Never open attachments, click on links, or respond to e-mails from suspicious or unknown senders.
- Gazprombank will never request you to provide sensitive information such as Password or PIN code by e-mail.
- If you have responded to a phishing e-mail with personal or account information, contact the Bank immediately.