

These General Terms and Conditions for the Use of i-bank services of Stopanska Banka AD – Skopje (hereinafter referred to as the General Terms and Conditions) regulate the mutual rights, obligations and responsibilities of the legal entity user (hereinafter referred to as the User) and Stopanska Banka AD – Skopje (hereinafter referred to as the Bank) relating to the use of i-Bank service of the Bank. The General Terms and Conditions for Use of i-bank service of the Bank shall be an integral part of the Framework Agreement of Payment Services concluded between the Bank and the User.

## 1. DEFINITIONS

1.1 The terms used in these General Terms and Conditions shall have the following meaning:

- **I-bank service** shall mean the name of the digital bank service platform of Stopanska Banka AD – Skopje through which the Bank provides online payment service relating to payment account via the Internet and/or mobile application. It is a system of modern channels through which banking services and products are offered via interactive electronic communication channels.
- **I-bank service user** shall mean an authorized person of the legal entity registered in the Bank that at least has one payment account in the Bank.
- **Username** shall mean a unique name assigned by the Bank to the User's authorized person for operating the accounts allowing access to i-bank service in combination with their password.
- **User password** shall mean a set of alphanumeric characters and numbers that, in combination with the Username, allow the User's authorized person to uniquely identify their access to i-bank Service of the Bank.
- **User access** shall mean a personalized device of authenticating the User exclusively for communication in a closed system for using i-bank Service.
- **Digital certificate** shall mean a file by which the signatory's electronic identity is determined.
- **PIN** shall mean a password provided by the issuer of the digital certificate to the User, which activates the certificate at the time of signing the order.
- **OTP Token** shall mean a personalized device, uniquely connected to the User, on which time-limited passwords are generated for identification of the User and authorization of payments and other services performed through i-bank Service. OTP token can be in physical or virtual (software) form.
- **Authorization and authentication** shall mean a process through which the Bank, through the assigned user accesses, unequivocally and digitally confirms the identity and consent of the User of i-Bank Service for the execution of payment orders enabled through i-bank Service or the use of certain services. Authentication of the User's identity is performed using a combination of personalized security tools (User Approaches) that include knowledge, possession and / or inheritance.
- **Mobile application** shall mean a software application installed on the user's device (mobile phone, tablet, etc.) through which the User accesses the Bank's mobile banking services.
- **Identification number (ID number)** shall mean a unique identification number of the User in the Bank's systems (generated by the Bank's core system).

## 2. SERVICE DESCRIPTION

2.1 Through i-Bank Service for legal entities of the Bank – registered clients of the Bank, as a service provider, the Bank shall allow the User the following:

- User access,
- Issue of digital certificate of the Bank, or acceptance of the digital certificate issued by an authorized issuer of certificates for use of the Bank's electronic banking,
- Activation and enabling use of a software token,

- Insight in the payment account/s balance of the Bank's User,
- Making payment transactions allowed by the Bank, within the limit defined, and
- Information and reports related to the User's banking services.

2.2 The services referred to in point 2.1 shall be allowed to the legal representative and/or the authorized persons of the User (hereinafter collectively referred to as the User's authorized persons) for operating the payment accounts. The services referred to in point 2.1 may be used by the User via the following one and/or two channels:

- **electronic banking (e-banking)**, available through the Bank's website, and
- **mobile banking (m-banking)**, available via the Bank's mobile application.

### 3. REGISTRATION / APPLICATION FORM FOR USE OF THE PAYMENT SERVICE

3.1 I-Bank Service User may be a resident legal entity, a registered client of the Bank, and as an exception, the Bank may approve the use of i-bank payment service (with limited functions) by a non-resident legal entity.

3.2 The User shall register to use i-Bank Service of the Bank by submitting and signing a Registration Form in the Bank's branches by an authorized / responsible person with the legal entity.

3.3 The User chooses one of the accesses offered by the Bank (hereinafter referred to as the User Access) for each authorized person of the User to operate the account:

- partial view-only access for insight and/or generating an order,
- full access for signing payments, and
- other User-specific type.

3.4 The Bank, based on the requested access, may assign to the User one or more personalized security device used to confirm payments and other financial services through i-Bank Service, as follows:

- Username and password,
- Digital certificate of the Bank,
- PIN code,
- OTP Token,
- Another device for authentication of payments and other services allowed through i-Bank Service, and
- Acceptance of a digital certificate of payments via i-Bank Service, issued by an authorized issuer.

3.5 The Bank shall assign a user name and initial password to the User or to the User's authorized persons for using the Bank's electronic and mobile banking services. Through the User name and password (a set of characters known only to the User) and through the Bank's digital certificate or the digital certificate issued by another authorized Certificate Issuer or software token or other device (electronic card, key and/or unique physical characteristics in accordance with the applicable regulation) only possessed by the User, i.e. the authorized persons of the User, the Bank confirms their identity and validates them as the only user of the service.

3.6 The User Accesses assigned is personalized security devices for authentication of the User and exclusively for communication in a closed system, that is, between the User and the Bank, and they shall not be valid and may not be used for communication in other systems without permission of the Bank.

## **4. INSTALLATION AND USE**

### **4.1 ELECTRONIC BANKING**

- 4.1.1 To use the Electronic Banking Service, the Bank shall provide the User installation software in electronic form that allows payment with a digital certificate issued on a USB token. The User shall independently install the software required for signing in line with installation Instructions available on the Bank's website.
- 4.1.2 The Bank, at the User's request, may issue a digital certificate accepted in i-Bank Service of the Bank, or allow acceptance of a digital certificate issued by an authorized Certificate Issuer for use of the Bank's electronic banking. The Bank shall issue to the User a digital certificate for the User's authorized persons to operate the payment accounts exclusively for the use of Electronic Banking Services, and it may not be used for communication in other systems outside the Bank.
- 4.1.3 For use of the digital certificate the Bank shall assign a Password - PIN for activation of the certificate at the time of signing an order.
- 4.1.4 The digital certificate shall be assigned with a validity period determined by the Certificate Issuer and the User of i-bank Service shall be obliged to be informed in a timely manner on its validity and ensure its timely renewal for uninterrupted continuation of the use of i-Bank Service.
- 4.1.5 In addition to the electronic banking, the User shall use mobile banking of the Bank, and may use the issued software OTP token for signing payment orders through electronic banking. In such a way, the User that has been issued a software OTP token through the Bank's mobile application creates a payment code that will be further used for authentication every time the software OTP token is used to sign orders through electronic banking.

### **4.2 MOBILE BANKING**

- 4.2.1 To use the mobile banking service, the Bank allows the User to activate a software OTP token for payments through mobile banking (m-banking) on the Bank's mobile application.
- 4.2.2 The Bank shall activate software OTP token to the User for the devices on which the software token shall be installed and for the authorized persons of the User to work with the payment accounts that will use the software token, exclusively for the use of mobile banking services and it may not be used for communication in other systems outside the Bank.
- 4.2.3 The User shall independently download and installs the Bank's mobile application available for IOS and Android devices and activate the software token with the activation code provided by the Bank in accordance with the Instructions for Activation and use of the software token available on the Bank's website.
- 4.2.4 Through the Bank's mobile application, the User shall create a payment code that will be used for authentication every time the software OTP token is used for signing orders through mobile or electronic banking.
- 4.2.5 The software token shall be provided for an indefinite time. In case of change of the validity time of the software token in accordance with the Bank's business policy and internal acts, the Bank shall be obliged to immediately notify the User.

### 4.3 TERMS AND CONDITIONS TIME SCHEDULE AND COSTS OF USE

- 4.3.1 The Bank shall undertake to ensure timely execution of all correctly completed bank transaction orders submitted within the terms published in the Bank's Time Schedule published at the Bank's counters and website: [www.stb.com.mk](http://www.stb.com.mk). The working days and hours for making payment transactions are determined by the Time Schedule that the Bank publishes on its website ([www.stb.com.mk](http://www.stb.com.mk)).
- 4.3.2 Each payment transaction made by the User through i-bank service is confirmed with a password to activate the digital certificate and/or software token or other device. Such payment transactions made shall be irrevocable and the Bank shall provide appropriate audit trails thereof kept in accordance with the applicable laws and regulations.
- 4.3.3 The Bank shall not execute a payment transaction order if the User's account is frozen. The Bank shall not execute a payment order if the User's account does not have enough funds to execute the order or there are not enough funds to pay the Bank's commission, or if the execution of the order would exceed the allowed overdraft of the account. The Bank shall not execute a payment order if the User's data and documents are not updated in accordance with applicable laws and regulations and the Bank's internal acts.
- 4.3.4 The Bank shall not be responsible if the Bank was unable to execute or is in delay of executing the payment through electronic banking due to any of the following reasons:
- events beyond the control of the Bank occur due to force majeure, loss of telecommunication connections, fire, flood, viruses, etc., which may delay the execution of the order;
  - the equipment and/or software of the User or the Bank do not work, and the User knew or was notified by the Bank about the problem or interruption in operation before trying to issue a payment order;
  - if the party in whose favor the payment is made is unable to accept the payment or otherwise causes a delay in the transfer of funds; and
  - if the User has not submitted appropriate documentation for the payment in accordance with the applicable laws and regulations and the Bank's internal acts or if the payment exceeds the defined payment limits according to the internal acts of the Bank.
- 4.3.5 The Bank shall calculate and collect the costs for the purchase of a bearer certificate and the costs incurred for using i-bank service from the User's account, in accordance with the applicable Service Fee Tariffs published on the Bank's website: [www.stb.com.mk](http://www.stb.com.mk).
- 4.3.6 The User agrees to be informed about the type and amount of costs incurred for using the Bank's i-bank service from the notices at the Bank's counters and/or the Bank's website.
- 4.3.7 The User authorizes the Bank to debit the User's account to collect the above costs. If there are no funds on the account from which the payment is made, the User authorizes the Bank to charge the incurred costs for using the services against the tacit debit balance that the User agrees to be made available by the Bank for that purpose or by seizing of funds, i.e. issuance of payment instruments charged to any account of the User in the Bank.

## 5 RIGHTS AND OBLIGATIONS OF THE USER

- 5.1 The User may only use the Bank's i-bank service if the User possesses a generated and personalized digital certificate or software token or device (electronic card, key, and/or unique physical characteristics in accordance with the applicable regulation) issued to the User's authorized persons in their exclusive possession and connected to the URN and TIN of the User-legal entity.
- 5.2 The User shall be obliged to provide to the Bank personal data, required for personalization and generation of the certificate and/or for activation of the software token, of all authorized persons who shall make payments and transfers in and on behalf of the User through the Bank's i-bank service by securing the authorized person's consent.
- 5.3 The User shall undertake to, in case of change in the personal data of the persons authorized to make payments and transfers in and on behalf of the User, immediately notify the Bank in writing thereof. The Bank shall not assume any responsibilities for payment and transfers made by a person(s) that was replaced, in the period from his/her change to the time of receipt of the written notification by the Bank.
- 5.4 The User shall undertake to ensure that their authorized persons treat the password, certificate and device on which the software token is activated as confidential information, not to disclose them to third parties and not to allow a third party:
- to use the User's name in the i-bank service of the Bank,
  - to have access to the User's account(s), and
  - to make transactions from the User's account.
- 5.5 The User shall undertake to ensure that their authorized persons take all necessary actions to keep confidential the password, certificate and device on which the software token is activated and to prevent any unauthorized access to the data and electronic signature devices as well as to log off from the web access to the Bank's i-bank service whenever physically leaving the computer, i.e. to log out of the Bank's mobile application after using mobile banking.
- 5.6 In case the User fails to comply with the assumed obligations, the Bank shall not bear any responsibility.
- 5.7 The User authorizes the Bank to realize any message signed electronically by the User's authorized persons.
- 5.8 Any message signed by the authorized persons of the User with their electronic signature certificate/OTP token shall be irrevocable.
- 5.9 The User shall undertake to, after each given transaction order, obligatory check whether it has been executed and, if not, to ascertain whether there is a reason for the non-execution of the payment.
- 5.10 The User shall undertake to notify the Bank immediately if the User suspects that the Bank's digital certificate, software token and/or the password of any authorized person to make transactions or transfers in and on behalf of the User have been compromised or misused or that a third party has used or attempted to use them without the User's consent.

5.11 The User shall undertake to notify the Bank immediately if any of the User's authorized persons to make transactions or transfers in and on behalf of the User has lost the digital certificate and/or password and/or software token, i.e. a device on which software token or other device is activated, or has been stolen.

## **6 FINAL PROVISIONS**

6.1 The Bank shall reserve the right to make changes in the offer and contents of some services and functions of electronic and mobile banking regulated under the Framework Agreement of Payment Services and these General Terms and Conditions.

6.2 The Bank shall propose to the User any amendments to these General Terms and Conditions not later than two months before the date of their application in one of the following manners: 1) through a written notification, 2) via electronic mail, or 3) by publishing it on the Bank's website.

6.3 The User shall have the right to accept or refuse the proposed amendments referred to in point 6.1 prior to the date of application of the amendments and notify the Bank thereof.

6.4 If the User fails to notify the Bank that they do not accept the proposed amendments before the date of their application, it shall be deemed that the User accepts the amendments proposed.

6.5 In case the User does not accept the proposed amendments, it shall be considered that User has submitted a request to discontinue using i-bank services of the Bank, i.e. requests to stop using the online payment service linked to the payment account.

6.6 The User agrees and is informed that the Bank may unilaterally and without prior notice temporarily or permanently limit the User's access to i-bank service at any time, if the Bank suspects that there is a possible misuse (by the User or by a third party) of the User Access or possible intentional or negligent inducement to improper operation of individual systems in the Bank or of the payment system as a whole.

6.7 The User agrees that the Bank may unilaterally and without prior notice temporarily or permanently limit his access to i-bank service, if the User has due and outstanding debt related to the use of i-bank service or other banking products and services.

6.8 The Bank may unilaterally exclude the User from i-bank service if, according to its own conviction, the Bank considers that the User intentionally or with gross negligence caused improper operation of the system for electronic banking, mobile banking and the payment system as a whole, as well as due to actions by the User not complying with the obligations assumed under, and non-compliance with these General Terms and Conditions.

6.9 In case of cancellation of the use of i-bank service for any reason, payment orders submitted before the cancellation, and with a future execution date shall be considered invalid.

6.10 The Bank shall not assume any responsibilities for direct or indirect events due to non-compliance by the User with the provisions of the Framework Agreement of Payment Services and these General Terms and Conditions.

6.11 These General Terms and Conditions shall apply as of 01.01.2023.