

## **SAFETY RECOMMENDATIONS OF TOKUDA BANK**

Using the system Online Banking, Tokuda Bank ensures maximum protection for your data and all transactions by implementing the following means:

### **I. Protected connection**

Access to the servers of Online Banking is carried out by encrypted https protocol. We use server certificate, issued by THAWTE Company, which guarantees the identity of the server the customers are linked to.

### **II. Signature of transactions by TAN (transaction authorization number).**

The TAN is a unique, one-time valid 6-digit code used, which is identification password sent via sms. The generated TAN password is valid for a limited period of time and can be used only once. With one TAN a document or group of documents can be signed or sent to the Bank. The Bank and Client or the Bank and the User shall agree that the TAN via sms shall represent an authorized electronic signature and as such they shall agree that they recognise the TAN via sms as a personal signature. They should have a registered phone number in the Bank system. Each user is responsible personally for TAN safekeeping.

### **III. Username and password.**

Each user of the system has a unique name and password known only to him. It is recommended that upon first log-in users change their password.

Tokuda Bank applies professional security measures for protecting its computer net. Nevertheless, when using Online Banking, it is very important to use the security measures for protection of your computers and computer nets. Therefore, we recommend the following **security measures** to be used:

- A. Keep your username and password, never write them on paper, disk, USB, etc. Do not write them in e-mails and do not give them to other people –they are personal!
- B. Use secured passwords, consisting of small and capital letters (e.g. a-z, A\_Z), punctuation marks and numbers (e.g. 0-9,!?"%=:/\_№@#\$\$%^&\*()\_+) which have at least 7 letters or/and digits and are not based on personal data, family names, etc. Periodically change your password for access (e.g. each 1-3 months).
- C. To access the system, always write in the address <https://rbank.tokudabank.bg/oraweb>. Check the communication protocol and be sure that <https://rbank.tokudabank.bg> has server certificate, issued by THAWTE.
- D. Do not use options for automatic save of user name and password.
- E. Always use the button EXIT after finishing work with the Internet Banking.
- F. Use only legal programs, purchased from suppliers who you trust. Update them regularly.
- G. We recommend to use anti-virus programs, which are regularly maintained and updated.
- H. Avoid using Online Banking from computers with unregulated access in the presence of other people. (Computer clubs, Internet cafes, libraries, etc.).