



~~MAYBE~~

MY SAFEST
INTERNETBANK

Let's start.  UniCredit Bank

“UniCredit Bank” places the highest emphasis on the security of direct banking products. The Bank implements UniCredit Group’s security standard that is developed by the Group’s professionals and is used across Europe.

When concluding agreement of Internetbank usage, the Bank assigns each user a User ID. In order to ensure security of data customer has to choose a security tool – either Security token or Mobile token.

SECURITY TOKEN

The Security token (also known as Code calculator) that generates unique (new) security code with each use is one of the highest security standards available today. It ensures secure login to Internetbank and secure authorization of transactions.

Security token’s PIN code

- PIN code is a combination of four digits, which is necessary to activate the Security token (see “Setup of new PIN”). PIN code should be kept in secret and it should never be disclosed to anyone, including Bank’s employees.
- In case the PIN code is discovered by third persons or in case of any suspicion that the PIN code is known to third persons, the User should change the PIN code immediately (see “Change of existing PIN”).
- When entering wrong PIN code an error message appears (FAIL 1). After the third consecutive unsuccessful attempt (FAIL 3) Security token is automatically blocked. In order to unblock the Security token the User has to contact Bank’s specialists by phone or come to the Bank personally taking personal identification documents with him/her.

Security code

- Security code (access/authorization code) is a combination of eight digits used for Internetbank access and for transaction authorization.
- Security code is generated automatically by the Security token after entering the PIN code and it is valid for approximately 30 seconds. It is not allowed to use one code repeatedly.


Usage of Security token

Security token is switched on/off with button .

Security token is switched off automatically in about 30 seconds.

Setup of new PIN

The new Security token you will get from the Bank will be without any PIN and you should set it up during your first access to Internetbank. In order to set up the PIN code:

- Switch on the Security token with button .
- You will see the message NEW PIN in Security token's display. Enter new PIN consisting of any 4 digits of your choice once.
- You will see the message PIN CONF in Security token's display. Confirm the PIN by entering your PIN code one more time.

You will not see the numbers in display while entering the PIN code in Security token. You should remember your PIN already by the first input. For security reasons it is not advised to make any remark of the PIN in written format.


Text in display	User actions
	Switch on Security token with 
NEW PIN - - - -	Enter the new PIN
- - - - PIN CONF	Repeat the new PIN
NEW PIN CONF	

Change of existing PIN

Text in display	User actions
	Switch on Security token with 
PIN - - - -	Enter your PIN
- - - -	Press and hold for approx. 2 seconds the button 
NEW PIN - - - -	Enter the new PIN
- - - - PIN CONF	Repeat the new PIN
NEW PIN CONF	

Generation of Security code

During login User should enter his/her User ID and Security code. Security code is used for login and for transaction authorization in Internetbank.

Text in display	User actions
	Switch on Security token with 
PIN - - - -	Enter your PIN
X X X X X X X X	The 8 digit long Security code will be displayed to the User. You should input this code into the field SECURITY CODE during login and when authorizing transactions in Internetbank.

MOBILE TOKEN

As alternative security tool for our customers the Bank offers usage of Mobile token. Mobile token gives more flexibility and freedom as the Security code is received in the mobile phone.

If a User has made a decision to use Mobile token, it is User's responsibility to provide the Bank with correct information about the mobile phone number to which Security code will be sent in the future. If the mobile phone number is changed or in case of loss or theft of the mobile phone it is User's responsibility to inform the Bank about the changes in due time by coming to the Bank personally. Changes will be incorporated into Internetbank's Usage Agreement and afterwards the Mobile security code will be sent to the new mobile phone number.

Mobile token's Password

In order to protect your Mobile security code, a password is used. Initial Password is provided by the Bank.

During first login, the system will initiate mandatory Password change. The new Password should be 6 – 10 characters long and should be entered twice – first time for setup and second time for confirmation. Once the new Password is entered twice, click on button CHANGE PASSWORD.

Generation of Mobile token code for login

During login User should enter his/her User ID and Password. Confirm your data by pressing button LOGIN. In next few seconds a message containing Mobile token code and short login information will be sent to Your mobile phone number.

Mobile token code should be input into the field MOBILE TOKEN CODE and confirmed by OK. Once the code expires, you should request a new code by clicking BACK and repeating login procedure.

Generation of Mobile token code for authorization

Mobile token code should be requested every time when the transaction authorization is performed. In order to receive the Mobile token code in your mobile phone, select the orders you are going to sign and click on button SEND ME TOKEN CODE. In few seconds a message with the Mobile token code and information about orders you want to sign with the code will be sent to Your mobile phone number.

The code is valid for selected transactions for approximately 20 seconds. Enter the Mobile code into the field MOBILE TOKEN and click on button SIGN. Once the code expires, you should request a new code.

Enter AS "UniCredit Bank" new Internetbank directly or via home page:
ee.unicreditbanking.net / lv.unicreditbanking.net / lt.unicreditbanking.net
www.unicreditbank.ee / www.unicreditbank.lv / www.unicreditbank.lt