RIETUMU

Application for iPhone and iPad iRietumu HD with integrated Digipass Mobile

Rietumu Bank launches a new application for mobile devices iPhone and iPad – iRietumu HD, which allows Clients to work with the bank comfortably and safely.

The new application provides the Client with access to information about his accounts (balances and statements), allows to make payments and conversion of transactions, as well as provides an opportunity for authorising orders which are awaiting to be signed.

The new solution is in conformity with latest technological requirements regarding reliability and safety for the remote control of an account, provides high-level information protection in combination with simple and convenient operation.

When developing the new application, special attention has been devoted to its ergonomics and comfort: with its help, the most complicated external payments can be made as easily as replenish your account.

It is also important that the new application supports scenarios when a client uses several different Rietumu ID packages for working with the Bank.

The specific feature of the new application is its latest virtual digipass – Digipass Mobile©. It is integrated with the application and provides a previously unseen level of convenience and safety during remote operations with bank accounts.

At the same time, the already active Rietumu ID packages can also be used to work with the application.

iRietumu HD

You can easily start working with the Bank via iRietumu HD.
You need to:

1. download the program

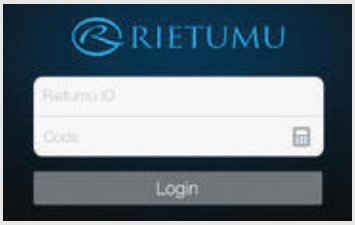
Download on the App Store

System Requirements:

- iPhone 4/4s/5/5s/6 or a later version
- iPad 2/3/4/Mini/Air or a later version
- OC: iOS 7 or a later version

2. open the program

3. enter your personal ID information



For identification in process of logging the system and signing all the orders and instructions you can :

- Rietumu ID and DigiPass OTP – pendant for logging in to the system and low-risk operations
- Rietumu ID and DigiPass DP 700 for all the operations
- Rietumu ID и DigiPass Mobile for all the operations

The Client receives his code for activating the Digipass Mobile in person, in a sealed PIN envelope. The code is presented in QR form and is a combination of symbols. The iRietumu HD application allows the activation code to be read and entered in the iPad by scanning the QR or manually.

The code for activating the Digipass Mobile can be received at the Headquarters or representative offices of the Bank.

The activation code can be ordered in person or via one's personal manager.

In the nearest future an application for receiving the Digipass Mobile code is planned to be submitted via the iRietumu remote access system.

Working with iRietumu HD and Digipass Mobile

- the most convenient way of working with your accounts

How Can the Application Be Installed and Activated?

Step 1:

Receive the Digipass Mobile code

Digipass Mobile is issued in the Bank or its regional representative offices

Step 2:

Install the iRietumu HD application on the iPhone/iPad

The iRietumu HD application can be found at the App Store

Step 3:

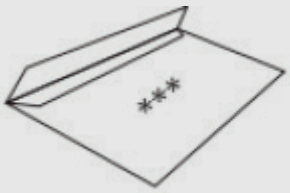
Start entering the Digipass Mobile code in the iPhone/iPad

Click on the Calculator icon in the password entry form and choose option "Scan QR Code"

Step 4:

Activate the Digipass Mobile

Scan the code or enter it manually. Invent and enter the name and access password for the Digipass Mobile. Contact the Bank to complete the activation



Download on the App Store

How to work with Digipass Mobile further on?

After the download and installation of the iRietumu HD application from the App Store, the virtual device Digipass Mobile will be available on all screens of the application via the Calculator icon.

Function of Digipass Mobile in one identical to DigiPass DP700, i.e. can generate:

- one-time passwords for identification of the Bank and signing of low-risk instructions,
- digital signature fot all the orders and instructions, incl. payments.

Virtual device Digipass Mobile can be used separately from iRietumu HD application.

What is the special safety feature of the new application?

We are certain that safety must have specific tangible forms. The Bank's Client should understand how the device looks, where it is located and how the device or the protection system operates. The Client should also be able to decide when his signature is sent to the Bank.

As world practice shows, the most widespread form of a malicious attack (which is hard to be arranged), when working with banks via the internet, is the replacement of the beneficiary's details at the time of payment sending. In this case, the Client assumes that his funds are remitted to the right address, however at the time of dispatch a virus changes the account details of the receiver, providing an account number of the hacker instead.

Such a threat is easily overcome by the "physical" digipass calculator DP700, which is well-known to our clients – it is fully separated from the computer and is independent from it. The Client enters several key parameters of his payment (his account number and the beneficiary's account number, the payment amount and currency) into the generator and receives a unique signature code for the specific transaction. If the details of the beneficiary are falsified as a result of a malicious attack, the payment will be declined by the Bank.

A similar principle has also been retained by the developers for the mobile digipass. The iRietumu HD application cannot

independently form (calculate) a digital code; it passes payment parameters into the virtual Digipass Mobile; in this case, the Client must make sure that all these data are correct. Having received the unique signature code for the specific transaction, the Client decides when to send it to the bank.

Similarly to the classical "physical" digipass calculator DP700, the mobile digipass Digipass Mobile has two operational modes:

I – the one-time password generation mode; it is used for low-risk operations when funds do not change their owner, like system entry, conversion, reloading of cards, etc.

S – the digital signature code generation mode according to the specific transaction parameters: the account number of the sender and the beneficiary, the amount and currency of payment – this mode is used for operations of higher risk; in this case, the Cient must be very careful and precise when entering the payment parameters into the device. The resulting code will be the signature code which allows only the amount indicated by the Client to be remitted, and only to the account indicated by him.

NB! The iRietumu HD application has several levels of encryption and data protection.

The virtual applications Digipass Mobile are individual and unique: they are attached to the specific device (for example, the Client's iPhone or iPad) during activation and further on, they cannot be transferred to another device, copied or extracted in any other way.

The Digipass Mobile is integrated and activated in strict compliance with the safety requirements of the supplier of authentication means, which is confirmed by the audit.

What is important to know when working with Digipass Mobile?

1. Requests for Digipass Mobile password:

1. Minimal password length – 8 symbols
2. To create a password, is essential to use symbols from minimum three of mentioned groups:
• Latin alphabet upper case letters – A, B, C...
• Latin alphabet lower case letters – a, b, c...
• numbers – 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
• special symbols – ` ~ ! @ # $ % ^ & * ( ) _ + = { } | : " ; ' < > ? , .
3. Forbidden symbols:
• gaps, hyphens, slash symbols
• any other alphabet letters apart from Latin
• words from dictionaries and proper names
• user's and his relatives and friends personal data (for example, names and surnames, phone numbers, dates of birth, addresses, work place names etc.)

"Keep me logged in" function

There is "Keep me logged in" function in the internet bank mobile version for client convenience. It allows to log in to the internet bank from your gadget in viewing mode without one-time password repeated request.

Please note that if using this function an authentication token will be kept on your gadget. Therefore, despite of all security measures, chances of illicit access in viewing mode increases.

2. Having lost his/her iPhone or iPad, the Client also loses the virtual digipass which is integrated with it.

The previously used digipass cannot be activated repeatedly. In

the event of loss, one should apply to the Bank and receive a new Digipass Mobile.

3. The virtual Digipass Mobile cannot be restored from reserve copies.

Digipass is real access to money. Therefore during activation it is very deeply integrated into the Client's device. If a situation occurs when the Client blocks or loses his virtual digipass, he should receive a new one.

4. The Client can always easily update iOS versions and iRietumu HD applications.

Updating of iOS versions and applications does not influence the operation of Digipass Mobile in any way.

5. Old virtual digipasses cannot be transferred to new devices.

When the Client acquires a new iPhone or iPad, he should receive and activate a new Digipass Mobile on it.

6. The activated virtual digipass is independent of the iRietumu HD application.

The virtual digipass is also retained in the Client's device following the deletion of the application from it. To fully delete the digipass from a device, a special operation from the launched iRietumu HD application should be performed.

7. The time on the Client's device must be set automatically.

The virtual digipass operates according to UTC time and easily adjusts during the transition from winter time to summer time and back; there are also no problems during the automatic change of time zones when travelling.

However, it is important to ascertain that the automatic setting of time is activated. See Settings→Main →Date and time→ Automatically = activated. If the time is set manually, the time zone should be correctly indicated and in no way may the clock be adjusted after activation of the digipass. A device with an incorrect clock will generate incorrect codes.