Guide to internetbanking activation and login

Table of contents

Safe internetbank usage

- Always open a new browser for internet based banking services. Enter your internet banking ID and password only on the login page, accessible by you from www.raiffeisen.hu website entered in the address bar of your browser. Do not use any link to navigate to the browser because if you are not in the right place, you might get phishing attacked by adding your identification and password.
- NEVER use your Raiffeisen internetbank when you get the link through SMS, email or from a social media side, not even when you got it from a trustful partner.
- Check the side's authenticity and encoding. You will see a padlock icon on the browser's bottom line/ in the top heading.

The authenticity of the webpage can easily be checked by the certificate.

You can get more information from the IX. chapter of the Electra user manual.

- Take care of and never tell anyone your SMS code that you get from the bank to activate your internet bank, your password and PIN code what you specified after you activated the service. Do not make any note about your identification data (to your computer or to your mobile device) that by falling into unauthorized hands allows access to banking services in your name. When your internet browser asks for permission to keep your password, do not accept it.
- Do not download unknown origin or unknown application (for example Anydesk, Teamviewer) to your phone or your computer and do not allow remote access to your device for unauthorized person. Your bank will not ask you for this in connection with a virus protection or any other legal issue.
- Always read carefully what you get in SMS from your bank.

We draw your attention to scams disguised as executive or business messages.
This kind of scam is when the company's financial officer is tricked into paying a false invoice or transferring money from the company's account.

Fraudsters call the employee on the phone or send him an e-mail, pretending to be a high-level manager of the company or a well-known supplier.
With to the instructions received, the company's officer transfers the money to the bank account managed by the fraudsters.

Be careful if:
Your supplier sends you an email that their previously used bank account number is being changed and they request that their invoices have to be settled to another bank account number.
A leader representing your supplier gets in contact with you who you never worked with before.
They ask you to work in a different method.

Be careful when you get an email or a phone call:
Always attentively check the email address when you manage confidential information or transfer money.
When you have doubts about a payment request, ask for a competent colleague to help.
Do not open any suspect link or appendix which comes with an email.
Be especially careful when your log in to your personal e-mail account from your company's computer.

The financial information is a value and treatment of it needs increased caution:
If there is doubt about a call or in connection with an email, ask for confirmation through a different channel.
Use public or other cost-reimbursed database for checking the supplier's data and to establish its authenticity.

In case of downloading Electra customer terminal and automated terminal (Hypex) you should take especial care of the following instructions:

- You should only download if the company's computer contains adequate password and virus protection.
- If you install it on a hard drive, it should be encrypted if possible.
- Do not use an open Wi-Fi connection while using electronic banking channels (for example restaurant, café, hotel hotspot).
- Updates of the operating system, used on the computer, must be up to date.

If you find that you have been a victim of fraud, please call your relationship manager or other bank contact immediately, or our bank's Fraud Prevention team, which is available **24 hours** a day, every day of the week, on the following phone number: **+36 1 486 5380**
Please pay extra attention to your banking and company details.

TECHNICAL REQUIREMENTS

The login page of the Raiffeisen Portal has been developed in order to enable our Customers to access the Bank's digital services (e.g. internetbank) quickly and simply. Certain electronic services of the Bank will become accessible from this one single platform. Raiffeisen Portal login identification will be used in the course of login to Raiffeisen DirektNet. The electronic services accessible from the Raiffeisen Portal can be seen in the User's Manual.
The electronic services accessible from the Raiffeisen Electra can be seen in the User's Manual.

Internet banking and digital functions work only if you have an active internet connection. Before using the Electra or the DirektNet or the Portal internet banking platform, please enable JavaScript in your browser.

If after reading the information included in this manual you should have further questions, please call **our telephone customer service** at phone number **06-80-488-588** (free in the case of calls within Hungary).

APPLYING FOR THE DIREKTNET INTERNET BANKING SERVICE

How can I apply for internet banking access if I already have a Raiffeisen account?

Please complete the application form, and send it to the following address: Raiffeisen Bank Zrt. Budapest Pf. 1700.

If you prefer to do the application in-person, please visit the Raiffeisen branch that is nearest to you.

In order to avoid waiting, you can make an appointment in advance by clicking here.

Please bring the following documents for the application:

- ID card
- address card

After the service has been set, you have to activate it with the one-time activation code sent to you in SMS.

How can I apply for internet banking access if I do not have a Raiffeisen account yet?

Please visit the Raiffeisen branch nearest to you.

In order to avoid waiting, you can make an appointment in advance by clicking here.

Please bring the following documents for the account opening:

- ID card and
- address card

We will help you to select the account type that is most favourable for you.

Simultaneously with the account opening, apply for DirektNet internet banking access.

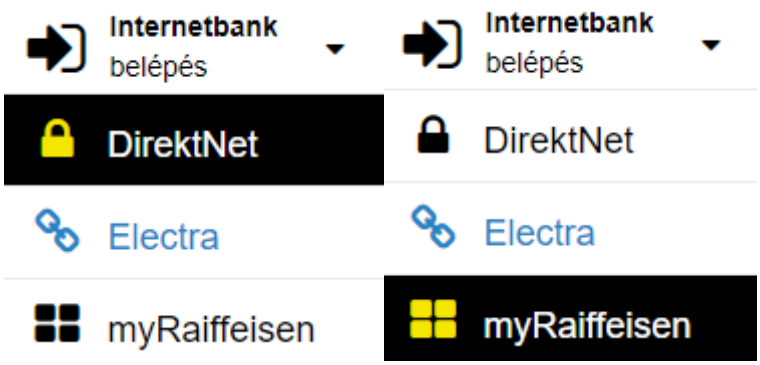
For the activation of DirektNet, a one-time activation code is sent to you in SMS, to the mobile phone number you have provided.

ACTIVATION

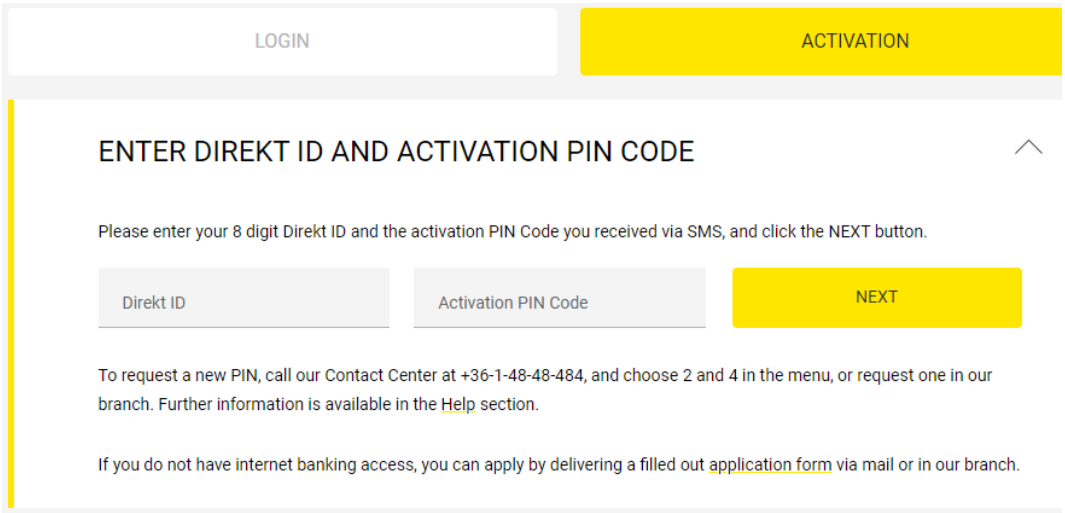
How can I activate my internet banking access?

Before using the system for the first time, you will **need to activate with the 8-digit Direkt ID** you received upon your DirektNet application and the **one-time activation code** got in SMS sent to your mobile phone number that you have identified and is included in the Bank's registry.

1. Open the website https://www.raiffeisen.hu/ in your browser,and click on the DirektNet or Portal option in the Internetbank login menu in the header.

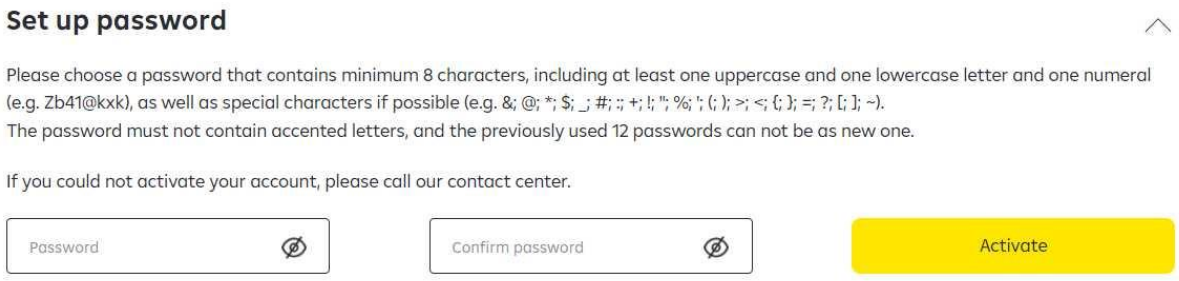


2. In the login page that opens up, click on the **ACTIVATION** tab, and enter your **Direkt ID** received from the Bank, and your **Activation PIN code** received in SMS, then click on the **NEXT** button.



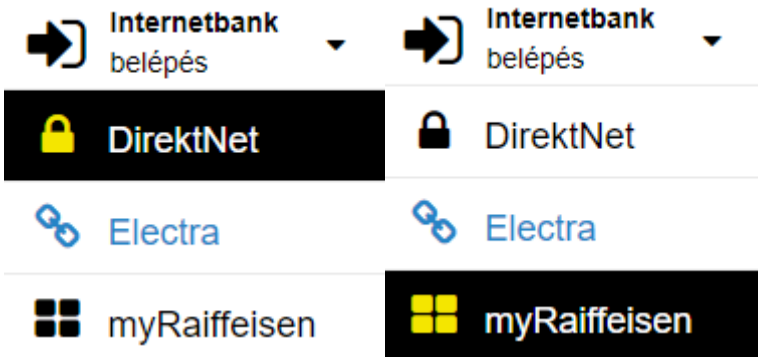
3. In the "**Password**" field, enter a password of your choice, which
   - should be minimum 8 character long
   - should include at least 1 lowercase letter,
   - should include at least 1 uppercase letter,
   - should include at least 1 numeral (e.g. Zb41jkxk),
   - should preferably include special characters as well (e.g. &, @, "),
   - must NOT include any accented letters.

After this, enter your password once again in the "**Confirm password**" field, then click on the **ACTIVATE** button. After successful activation, the page will offer login.



LOGIN

1. Open the website https://www.raiffeisen.hu/ in your browser, and click on the DirektNet or Portal option in the Internetbank login button in the header.



2. To log in on the LOGIN tab in the page that appears. After you have entered your Direkt ID, the system offers the following options for login:

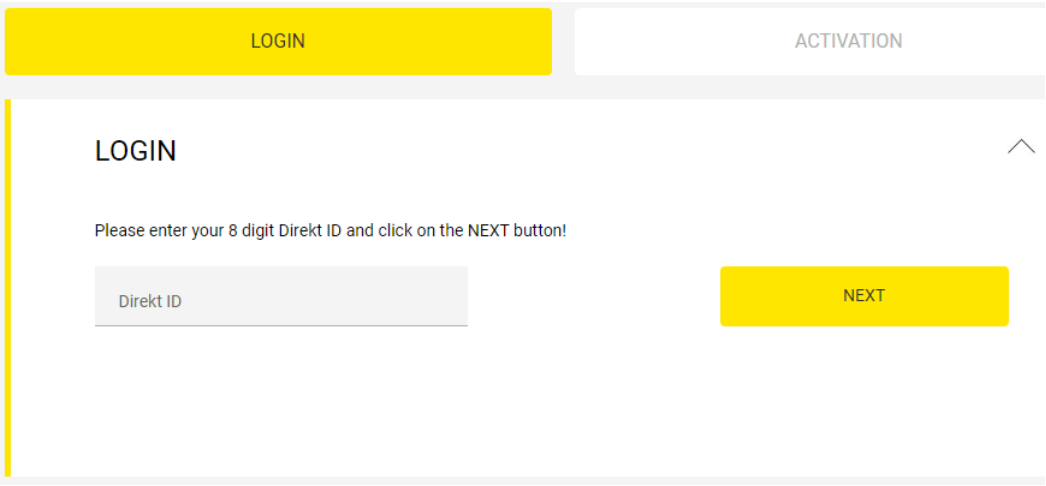
   - Login with Mobile token
   - Login with Hardware token
   - Login with password and SMS code

Login with Mobile token

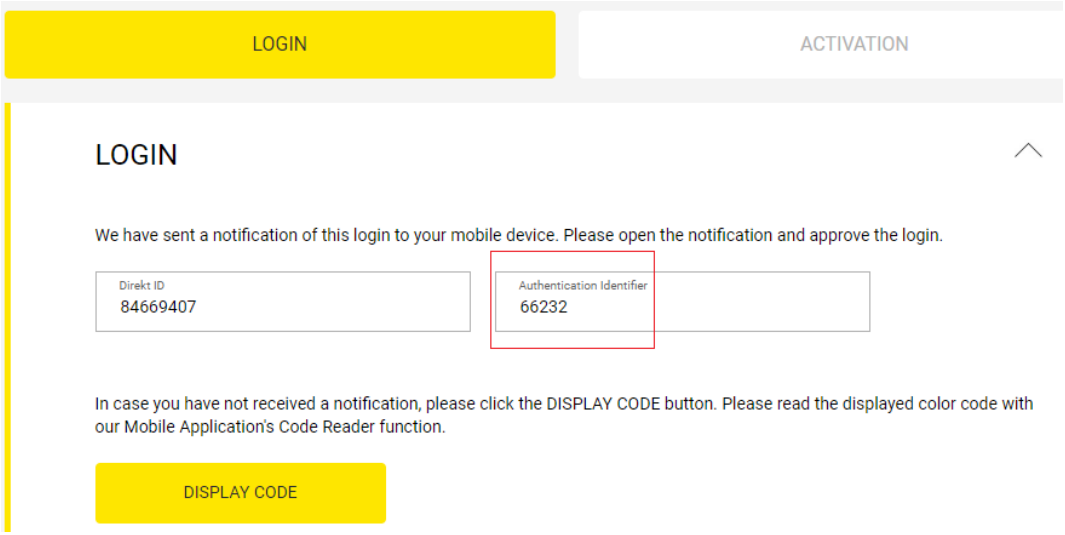
Mobile token is a high-security software authentication method built into myRaiffeisen mobile application to use DirektNet internet banking and mobile application services.

After entering your Direkt ID, you can approve the login in your mobile device. If you already use myRaiffeisen mobile application, the system will by default lead you through the process of login with Mobile token.

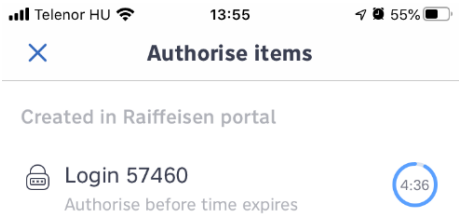
1. Please enter your **DirektNet ID**, then click on the **NEXT** button.



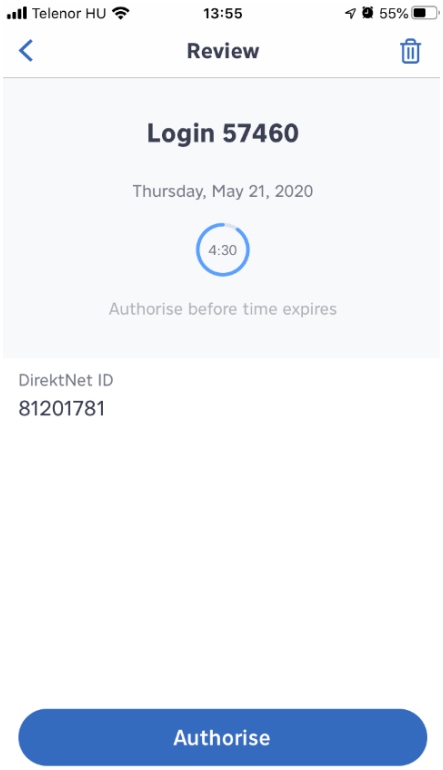
2. **Authentication code** field appears with an identification number. If you have **allowed push notifications** for the myRaiffeisen mobile application, you will receive a Push notification on the approval of login to your mobile device.



3. By pressing the Push notification, you can log in the application, and it will take you automatically to the "Sign transactions" page. Here can you see the login approval element (together with the transactions to be signed that were launched in the mobile application and in DirektNet).
4. Press the login approval element. You have 5 minutes for the approval (the time remaining is shown by the countdown clock).



5. Approve (authenticate) the login with the **Authorise** button.

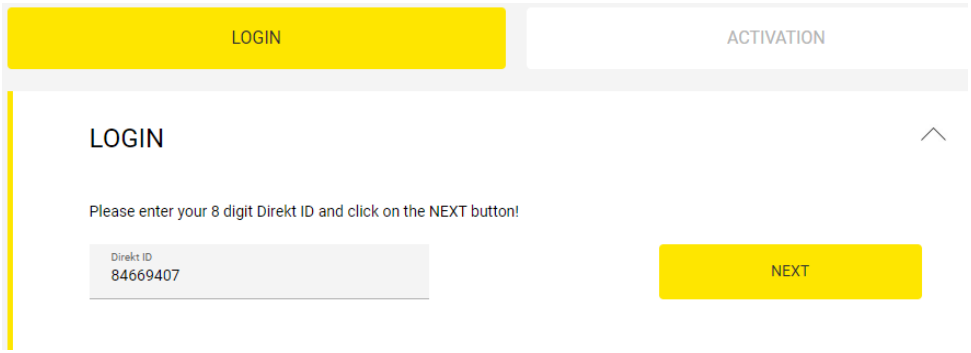


6. Depending on the Soft token settings you use,
   - enter your 5-digit PIN code, then press the "**Ok**" button, or
   - sign the login approval using fingerprint scan or Face ID.
7. After successful approval, within a few seconds the DirektNet home page appears.

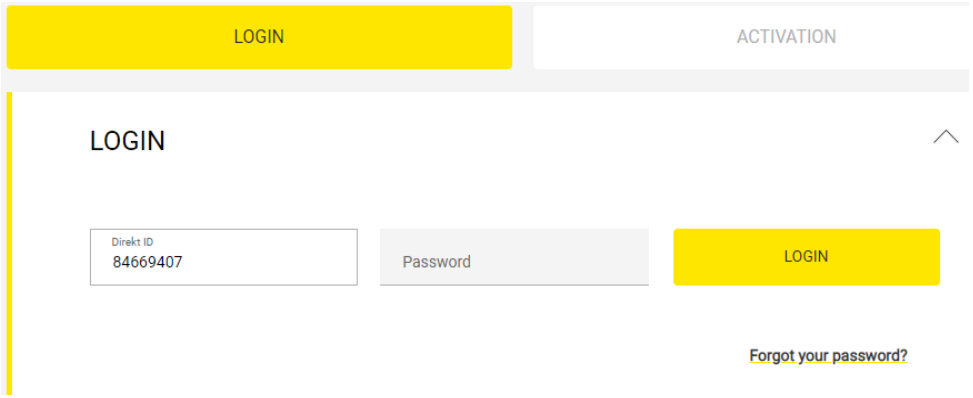
Login with password and SMS code

If you have not activated the Mobile token by activating myRaiffeisen application, and do not have a Hardware token either, you can log in by entering your Direkt ID, Password and a one-time login code sent in SMS to your device.

1. Please enter your DirektNet ID, then click on the **NEXT** button.



2. Enter your password in the **Password** field, then click on the **REQUEST CODE** button.

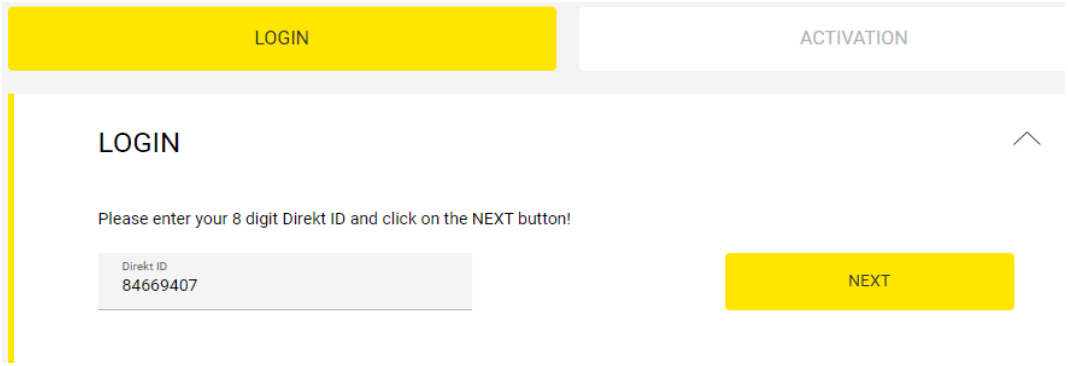


3. The one-time **activation code is sent to you in SMS, to the mobile phone number** that you have identified and is included in the Bank's registry. Please enter the code in the **SMS code** field, then click on the **LOGIN** button.

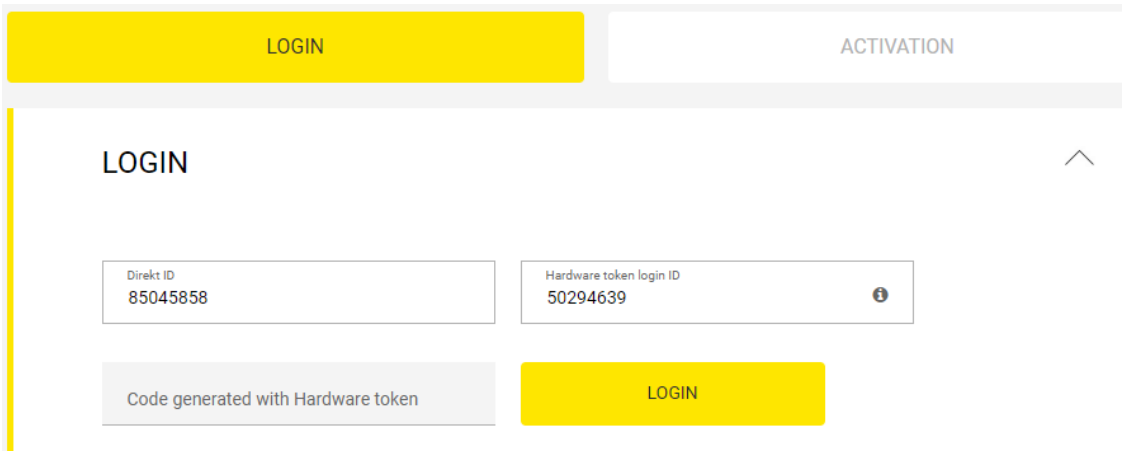
Login with Hardware token

If currently you use Hardware token to sign transactions, since April 2019 you may as well use this device to authenticate the login process.

1. Please enter your **8-digit Direkt ID** in the DirektNet ID field, then click on the **NEXT** button.



2. Please enter the generated code in the "**Code generated with Hardware token**" field, then click on the **LOGIN** button.



APPLYING FOR THE ELECTRA INTERNET BANKING SERVICE

How can I apply for Electra internet banking access if I already have a Raiffeisen account?

If your company's bank is Raiffeisen Bank, please contact your bank contact or advisor, who will conclude the contract with you.

For personal administration, please visit your bank contact or advisor and make an appointment with them!

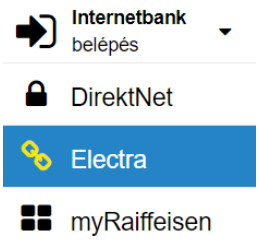
To apply and conclude a contract, you must provide the following information:

- Customer (Company) name
- Tax number
- For user(s): name, date of birth, mobile phone number

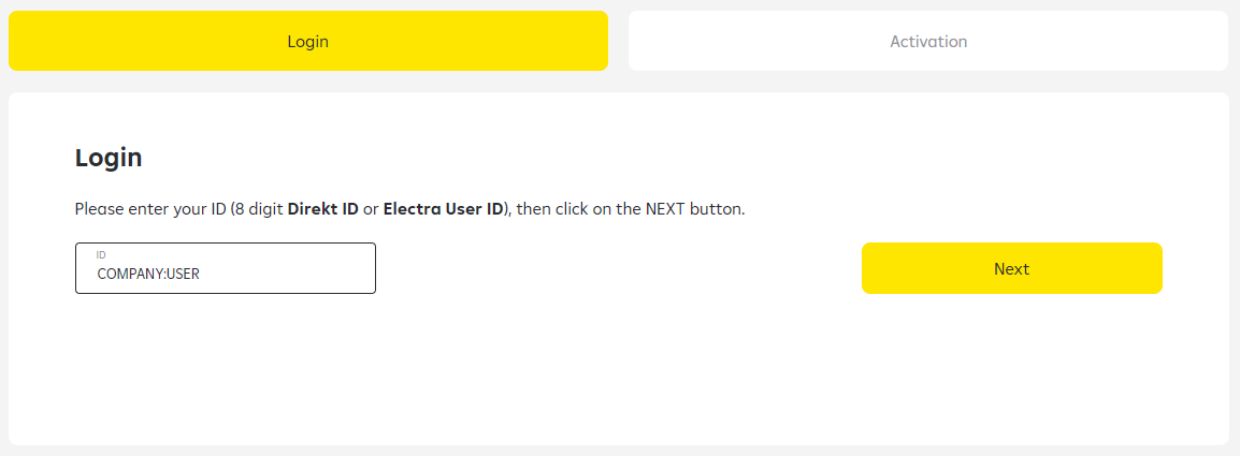
We set up the service for which we send the initial login password via SMS.

LOGIN

You can access Electra Internetbank from the home page of the https://www.raiffeisen.hu/ website by clicking on the **Electra** icon.



In all cases the login page is in the unitary Raiffeisen login screen, which you can find here: (https://sso.raiffeisen.hu/sso/XUI/#login/) In the login screen of Electra Internetbank, please enter your **Electra User ID**, then click on the **Next** button.



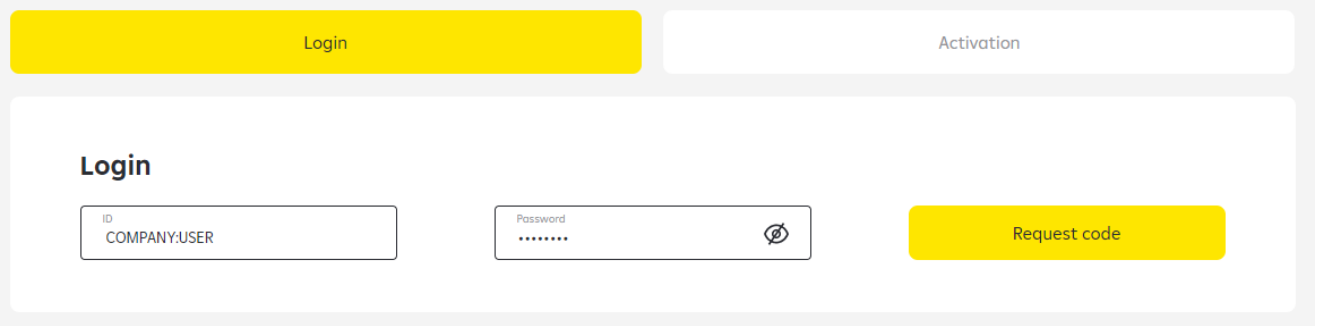
- **User ID:** the identifier provided in the Electra Request Form

The system will look after the User ID and the connected authentication method. You should have selected this in the Electra Request Form in your User data. According to this it will asks for data which required for identification.
The login process will be continuing by the following authentication methods:

- Login with password + SMS authentication method
- Login with Token authentication method
- Login with VICA mobilapplication authentication method

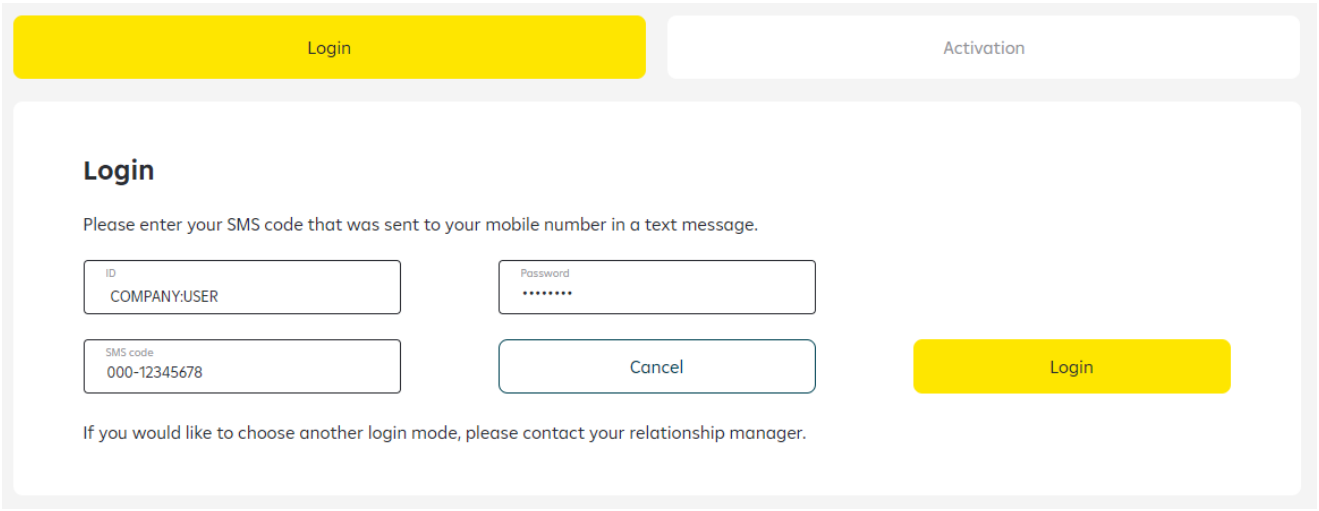
Login with password + SMS authentication method

In the password field you must enter your Login Password, then click to the „Request a code" button.



- **Login Password**: your Electra password received from the Bank in SMS or on a plastic card to be used for your first login

An SMS code will be arriving to your phone which will be needed for the authentication.You should enter this code into the right field than choose the „Login" button . With this you enter the Electra Internetbank starting page.

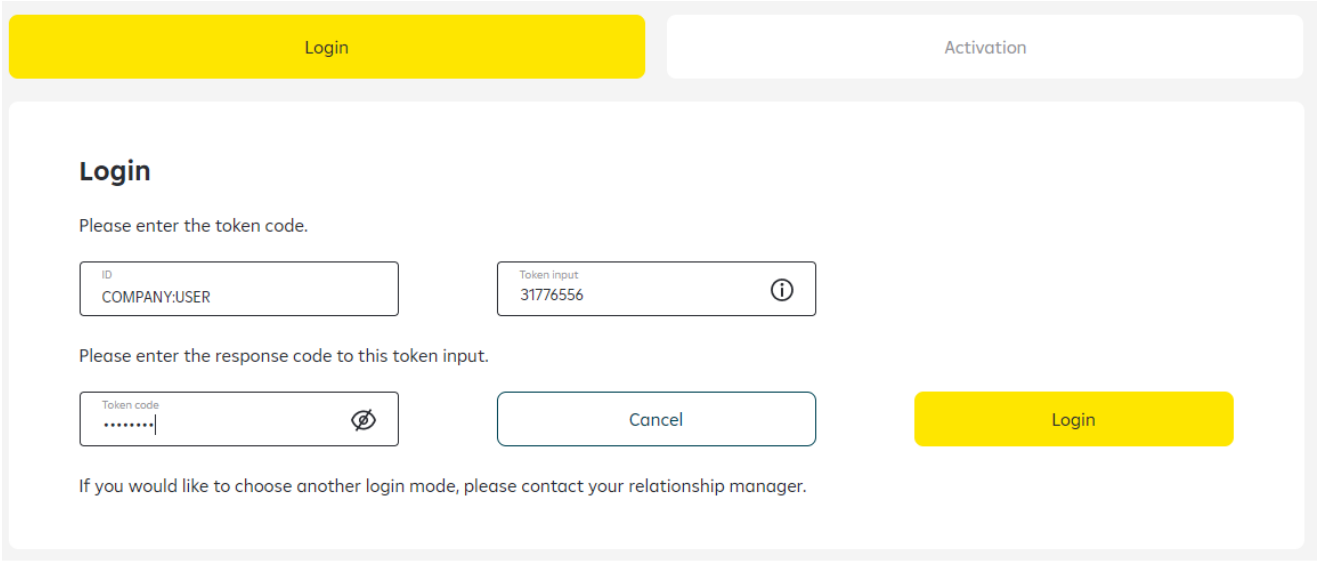


Your login password must be changed on a mandatory basis after your first login. To do so, you have to enter again your "old" password (that you received from the Bank for your first login), and have to provide your "new" **Login Password** selected by yourself, which can be validated by clicking on the **OK** button.

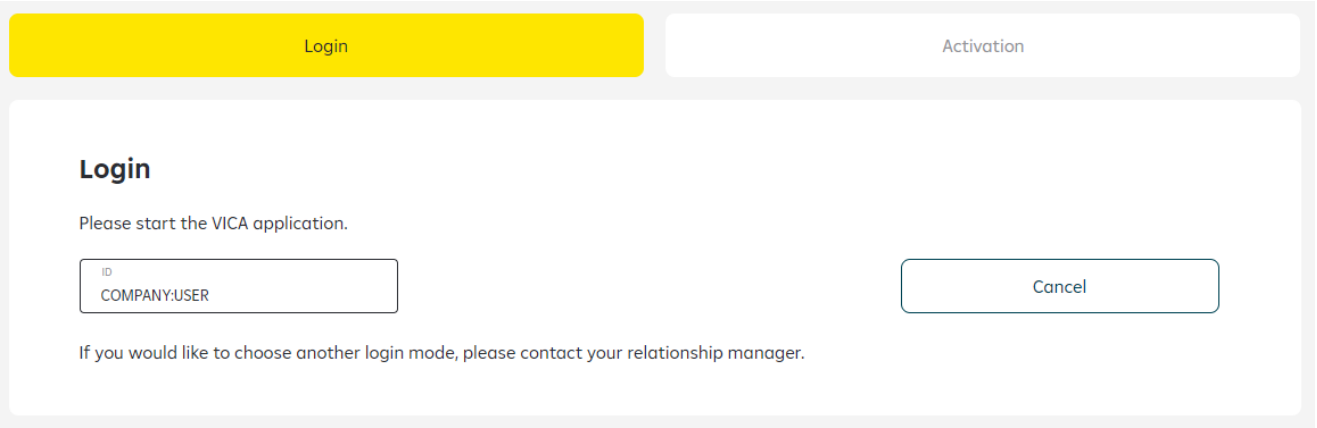
Login with Token authentication method

Turn on your signiture device (token) and sign in with your pin code, after you are done with that, you should type in the sequence of numbers you see in the Token input field.

You should type in your response code into the **Token code** field, then click on the **Login** button.



Login with VICA mobilapplication authentication method



Login to your ViCA application with the password, specified during registration, on your mobil phone.
After you have loged in, the next page will be a Raiffeisen Electra confirmation message.
The message include the user's name, the identification number and the date of the login.
In this screen if you click to the „Approval" button, the system will let you in to the Electra Internetbank's page, after that you can close the app in your mobile.