

Strong Customer Authentication in the OTPdirekt Electra Terminal Service

To ensure the security of electronic banking services, it is essential that the Bank provides appropriate protection against the misuse of customers' access credentials and the initiation of unauthorised transactions.

One of the most effective ways to enhance security is the use of Strong Customer Authentication (SCA). The Bank will soon make SCA mandatory for all users who have sole signing authority for a bank account and/or sole authority to represent a company.

Strong Customer Authentication requires customers to authenticate themselves using at least two independent authentication factors.

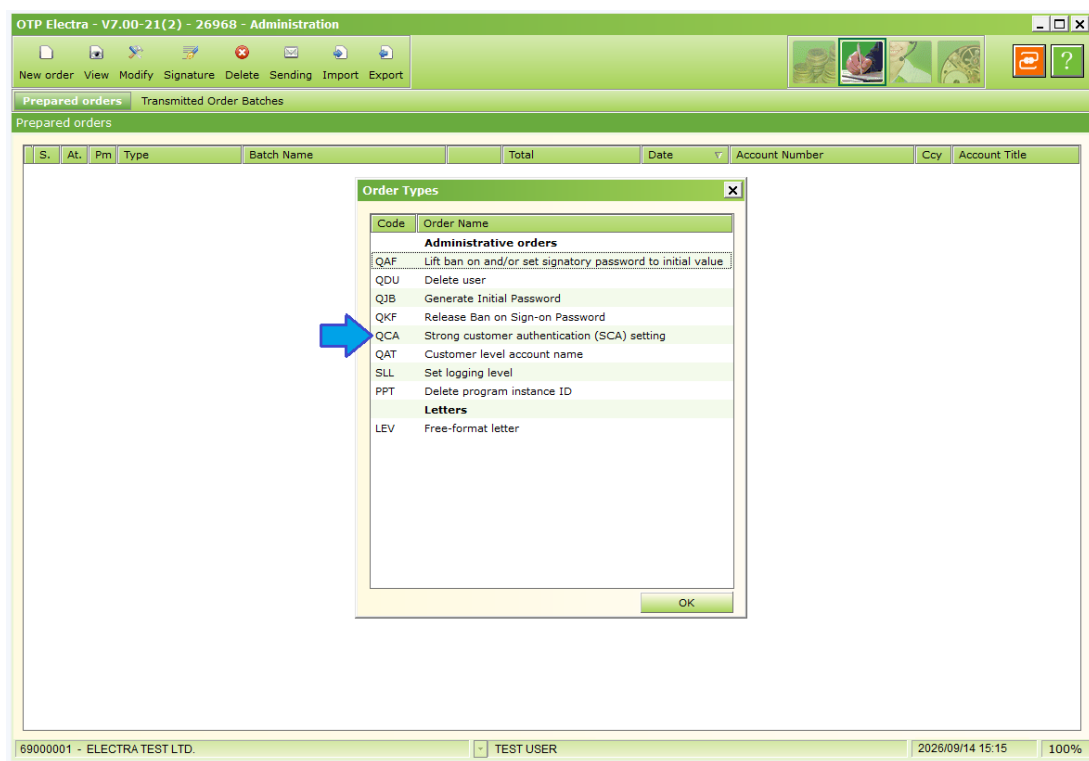
The Bank provides this two-factor authentication through the ViCA application.

The purpose of this document is to provide guidance to the users concerned on how to independently initiate the transition from password-based authentication to the ViCA authentication method.

Strong Customer Authentication Initiated from the OTPdirekt Electra Terminal steps for setting up ViCA

The OTPdirekt Electra Terminal client application, version 7.00-21, includes a new function in the Administration menu that enables users to switch from their current password-based authentication method to the ViCA authentication method.

In the *Prepared Orders / New Order* menu, the “QCA – Strong Customer Authentication (SCA) setting” command is available to all users who have signing authority for a bank account and/or authority to represent a company.



The user may only change their own authentication method. After logging in and initiating the creation of the package, it is advisable to verify the following information displayed on the screen:

- *User name,*
- *Date of birth,*
- *User Identifier,*
- *Customer authentication type.*

A Hungarian or foreign mobile phone number must be entered in the “*Mobile phone number*” field. To prevent typing errors, the same phone number must then be entered again in the “*Please enter Mobile phone number once again!*” field.

Strong customer authentication (SCA) setting

File Help

Save

Scheduled date
2026/09/14

User Name: TEST USER

Date of birth: 1962/08/18

User Identifier: TVICA : TESTUSER

Customer authentication type: VICA

An authentication code will be sent to verify the provided mobile phone number below.

Mobile phone number: +36-301234567

Please enter Mobile phone number once again!: +36-301234567

Validation

In the next step, the banking system will send an authentication code via SMS. The code must be entered in the “*Authentication code*” field of the “*Entering authentication code*” window, which will be displayed automatically.

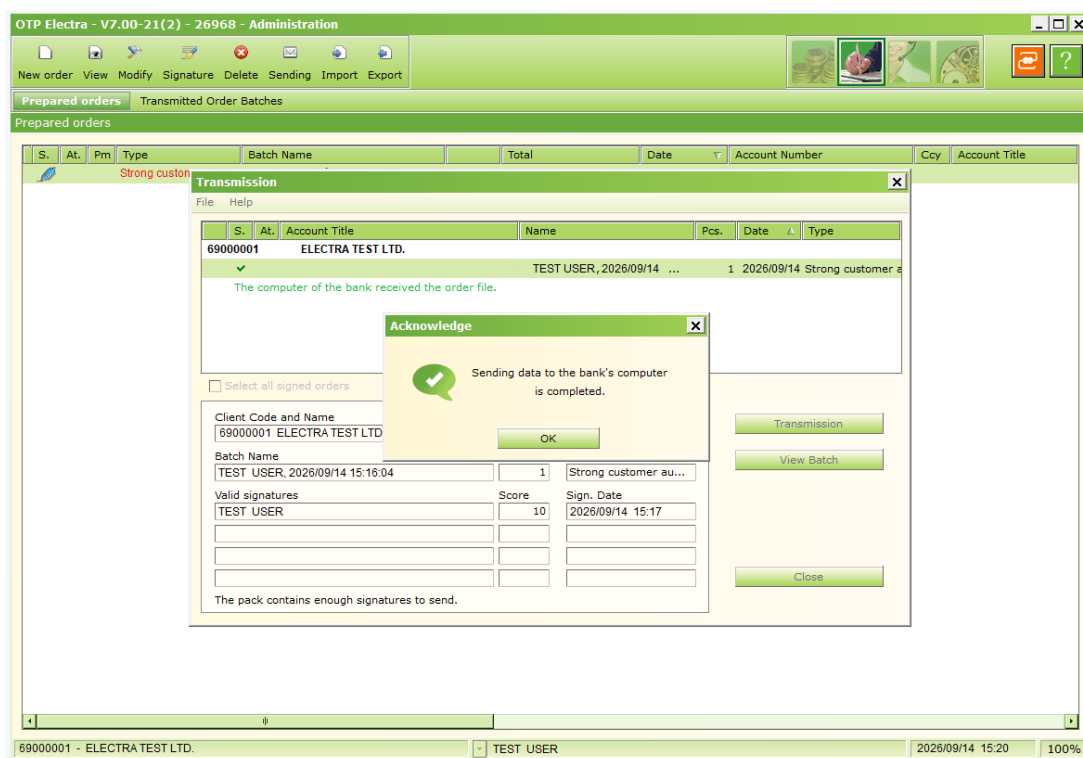
Entering authentication code

Type the authentication code received via text message.

Authentication code

OK Cancel

Following authentication, the “*Strong Customer Authentication (SCA) setting*” package created using the “*Save*” function must be signed individually by the user with their own signing password and submitted to the banking system.



Following the successful submission of the package, the banking system will send the ViCA registration code via SMS to the mobile phone number provided.

Using the code received, the ViCA application downloaded to the relevant mobile phone must be registered. The steps required to complete the registration are described in detail in the following guides:

- [ViCA Installation Guide for Android](#)
- [ViCA Installation Guide for iOS](#)

Further information on the ViCA service is available in the ViCA section of our [website](#) (Electra tab).

IMPORTANT!

- Upon successful submission of the “Strong Customer Authentication (SCA) Setup” package, the relevant user’s existing password-based authentication method will be changed to ViCA-based authentication. Consequently, the new authentication method will apply from the user’s next login. Registration of the ViCA ID is a prerequisite for using the system. Until registration has been completed, the user will not be able to log in to the Electra system or approve transaction packages, as password-based authentication will no longer be available.
- Local login cannot be initiated using the ViCA authentication method; it can only be used to log in to the Bank’s server.

Budapest, 8 October 2026



OTP Bank Nyrt.
 Postacím: 1876 Budapest
 Internet: www.otpbank.hu
 Társaság székhelye:
 1051 Budapest, Nádor utca 16.
 Fővárosi Bíróság, mint Cégbíróság:
 10-01-041585