

Roger Access Control System

Roger Mobile Key 3 Mobile App

Operating Manual

Software version: v3.0

Document version: Rev. B

The document is subject to the Terms of Use in the current version published at www.roger.pl.

INTENDED USE

Roger Mobile Key (RMK) is an application for Android and iOS mobile devices enabling the use of a portable device for the purpose of identifying users of the access control system. The users can be identified through the BLE, NFC (Android only), CLIP, and SMS technologies, or by displaying the QR graphic code on the mobile device's screen.

INSTALLATION AND CONFIGURATION

The Roger Mobile Key app requires Android 5.0/iOS 12.0 or later. The app for Android is available in Google Play Store and for iOS – in App Store. Once installed, the app is ready for configuration.

DESCRIPTION OF OPTIONS

Section: General settings

Command: Go to app settings

Selecting this parameter opens the application settings page in the Android/iOS system.

Command: Import settings from QR code

This option allows for importing the **Credential settings** from the QR code which can be scanned using a mobile phone camera. The QR code with settings may be generated in the RVDM program based on the settings of readers with mobile identification function.

Command: Restore to default

The setting restores the default setup of the **Credential settings**.

Section: Credential settings

Parameter: BLE factor class

The setting allows for selecting a BLE identification method, which will be used by the newly created key. The following options are available:

UCE – communication between mobile device and reader using the *challenge-response* method; means single-side authentication (the reader receives an acknowledgment that it communicates with the Roger Mobile Key app with a correct encryption password). The communication is encrypted using the AES128b standard. Identification with the UCE credential is faster than using the REK credential.

REK – communication between mobile device and reader takes place via safe communication channels using the *Encrypt-then-MAC* method with randomly generated keys. The communication is encrypted using the AES128b standard. Identification with the REK credential takes more time than using the UCE credential.

Note: Both methods are secured against transmission duplication, i.e., despite observation of data exchange, it is not possible to repeat communication to, e.g., gain access.

Parameter: NFC/BLE/QR code encryption key

The setting determines an encryption password for a key of the BLE, NFC (Android only), or QR type. Its value must correspond to the settings of the reader with which the key will be used.

Parameter: BLE communication encryption key

This setting specifies an encryption password for wireless communication to the reader. In most cases the password may remain default (the key relates to credentials added from the RMK app level).

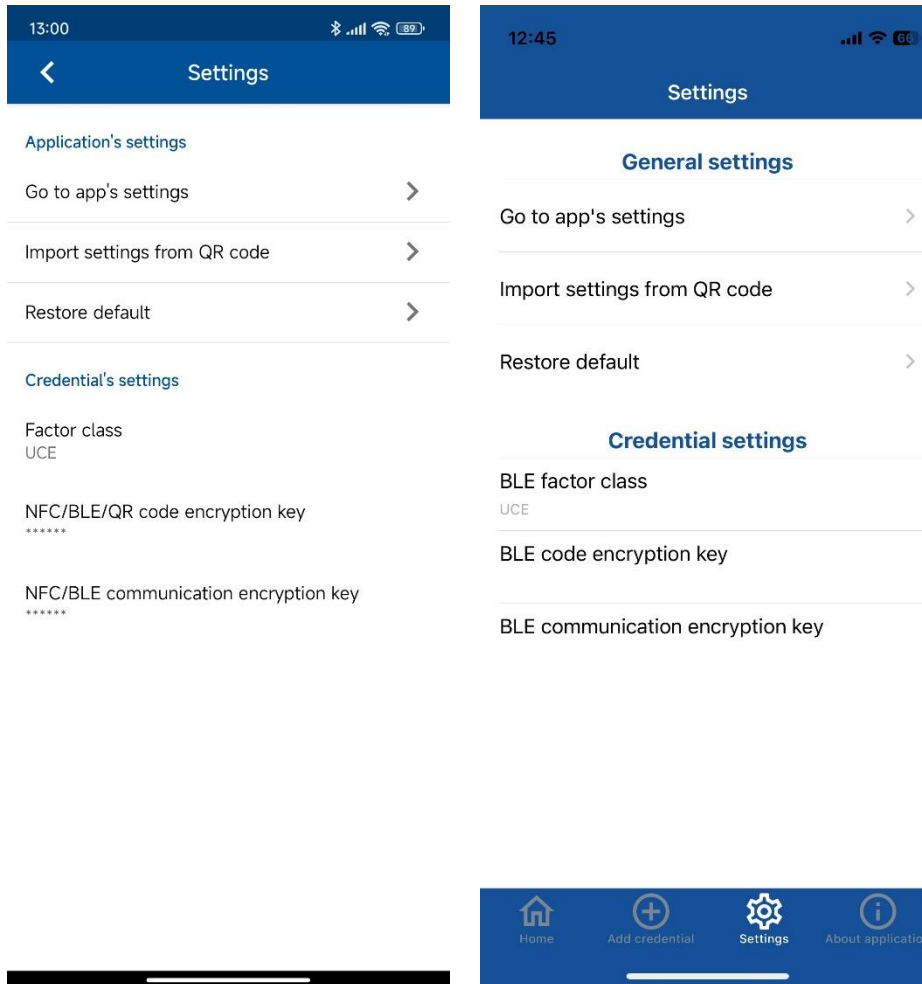



Fig. 1. App settings view (Android, iOS)

APP FUNCTIONS

Credentials

To create a new credential, click on the icon  (*Add credential*) and then specify the identification method (BLE, NFC, QR, PIN, CLIP, SMS), colour, name, and value. Once the credential is added, it will appear on the home screen.

NFC identification method is not available on iPhones.

PIN identification method is intended for ADL-2 locks.

CLIP and SMS identification methods are intended for the RCI-6 communication interface.

The RACS 5 system allows the users of the BLE, NFC, and QR credentials to create a mobile factor and share it from the QR code or .rek file level.

To add a credential from the QR code, click **ADD CREDENTIAL FROM QR CODE** and then scan the QR code provided by the system administrator. The app will display a window to enter the PIN code of the mobile factor and the BLE/NFC communication encryption key. If the access control system has keys defined, these need to be entered and the operation of adding a credential must be confirmed with the **OK** button.

To add a credential from the .rek file, open the received file using the RMK app. The app will display a window to enter the PIN code of the mobile factor and the BLE/NFC communication encryption key. If the access control system has keys defined, these need to be entered and the operation of adding a credential must be confirmed with the **OK** button.

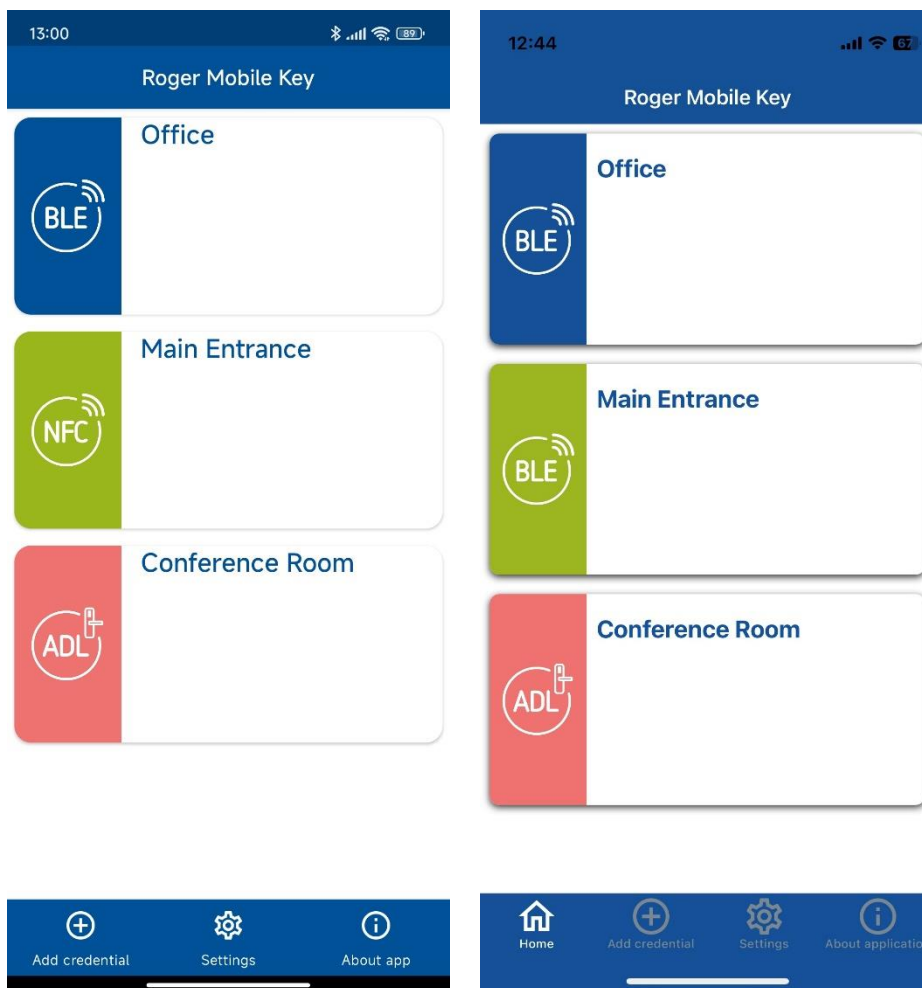


Fig. 2. App home screen (Android, iOS)

Key management

After adding the credential, the following operations will become available from the context menu by pressing and holding the credential:

Command: Assign paired readers

For BLE or PIN credentials, it is possible to specify one or multiple readers that the RMK application will prioritise when attempting connection. If only one reader has been specified, RMK will immediately start credential transmission to the reader, which significantly shortens the mobile identification process. When several paired readers have been specified, then only those readers will be available for selection when attempting to use the credential.

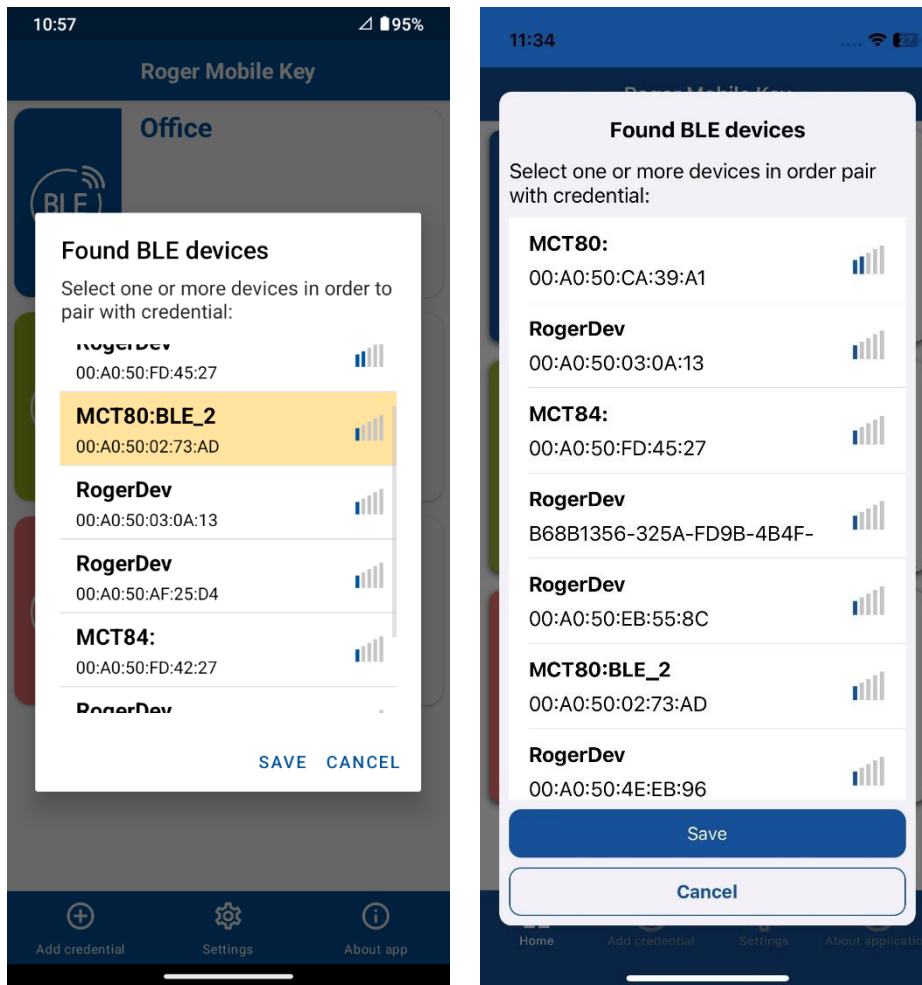


Fig. 3. View of the BLE readers found (Android, iOS)

Command: Edit credential

This option opens a window for editing the reader settings. It is possible to edit the description and colour, and a new factor value can be provided in the case of credentials defined on a mobile phone (and not imported from a QR code or e-mail attachment).

Command: Delete credential

Option for deleting a credential.

Using the credential

After clicking on the selected credential, the app, depending on the chosen communication channel, starts a communication process with access control terminal. Follow the description below as per the relevant credential type.

Credential type: BLE

Once you have clicked on the credential, the app shows the BLE readers found. To proceed to the authentication process, select the reader from the list. The login view will automatically close when the app gets an acknowledgment that the reader has received the data. The selection window will not show and RMK will automatically connect to the reader if only one paired reader has been defined for the credential or if one device from the group of paired readers is particularly close to the mobile phone, as evidenced by high signal strength.

Credential type: NFC (Android only)

After clicking on the credential, hold the mobile phone close to the front surface of the reader. Depending on the NFC antenna location in the mobile phone (typically the centre or top part of the

mobile phone back), it will be essential to select an optimal method for holding the device over the reader.

Credential type: QR

Once you have clicked on the credential, show the QR code to the reader's camera. The credential allows for changing the default size of the QR code. Default size is 10x10 mm. One click results in enlarging to 20x20 mm, while two clicks – to 40x40 mm.

Credential type: PIN

After clicking on the credential, the app will display the list of devices, which support remote PIN identification. To proceed to the authentication process, select the device from the list. The login view will close automatically when the application gets an acknowledgment that the reader has received the data, or if a connection error occurs. The selection window will not show and RMK will automatically connect to the reader if only one paired reader has been defined for the credential.

Credential type: CLIP

After clicking on the credential, a numeric keypad appears in the application to confirm a call to a predefined phone number.

Credential type: SMS

After clicking on the credential, the app will send an SMS to a predefined phone number.

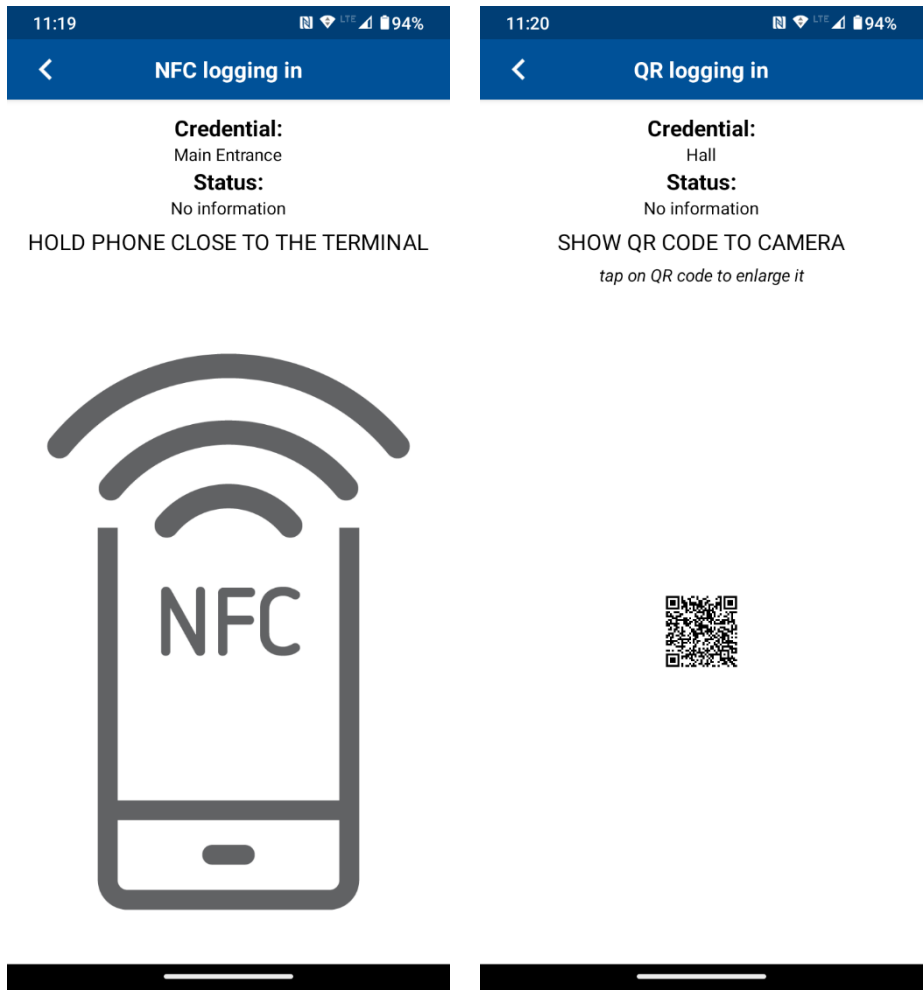


Fig. 4. Example screenshots during identification

Contact:

Roger sp. z o. o. sp. k.
82-400 Gościszewo 59
Tel: +48 55 272 0132
Fax: +48 55 272 0133
Technical support: +48 55 267 0126
Technical support (mob.): +48 664 294 087
E-mail: biuro@roger.pl
Web: <http://www.roger.pl>