Roger Access Control System 5

Application note no. 046

Document version: Rev. A

Users identification with mobile devices

Note: This document refers to RACS 5 v1.6.6 or higher

Introduction

Users can be identified in RACS 5 access control system by means of such Authentication Factors as proximity cards, PINs, fingerprints and also mobile devices with Android or iOS systems. The mobile identification can be in NFC (Near Field Communication) technology or BLE (Bluetooth Low Energy) technology on such terminals as MCT80M-BLE and MCT88M-IO which must be connected to MC16 access controller.

The solution enables to:

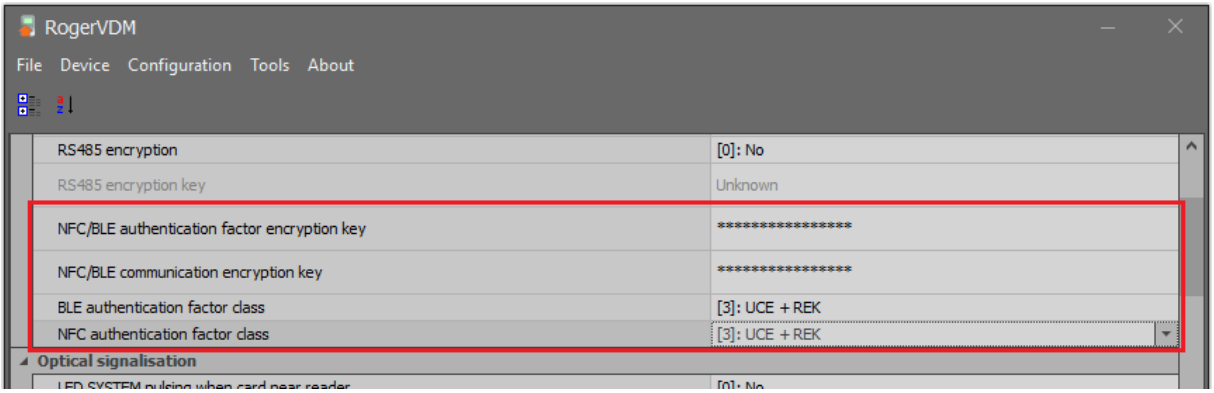
- Identify users via their mobiles devices with RMK app installed instead of or in parallel to proximity cards and/or other Authentication Factors.
- Identify users on MCT terminals by:
  - selection of credential on screen and then reading mobile device at the terminal (NFC)
  - selection of credential on screen and then reading mobile device in distance of up to 10 meters from the terminal (BLE)
  - making gesture with mobile device such as rotating and shaking (BLE)

In RACS 5 system, the identification of user including mobile identification at terminal can be used not only for access granting functions but also for other functions such as for example building automation.

Terminal configuration

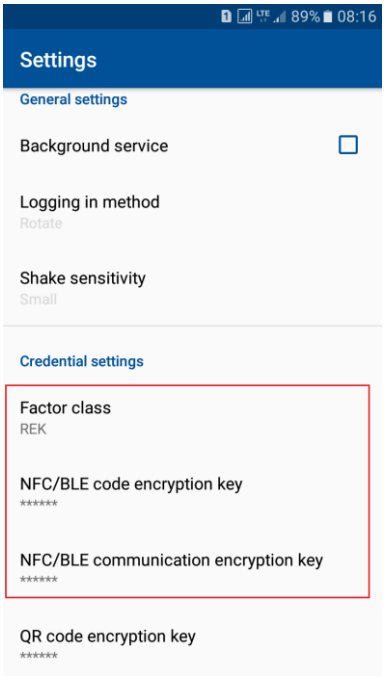
According to its installation manual, the low level configuration of MCT88M-IO and MCT80M-BLE terminals is conducted with RogerVDM software after their connection to computer via RUD-1 interface. In case of terminals for mobile identification except for typical addressing on RS485 bus it is possible to define such parameters as *NFC/BLE authentication factor encryption key* and *NFC/BLE communication encryption key*. Additionally factor class can be defined both for NFC and BLE. It is recommended to apply the option *[3]: UCE + REK* for both classes.

Note: If mobile factors are supposed to be defined based on further explained *.rmk files (method 2) then it is recommended to keep default empty *NFC/BLE communication encryption key* to simplify further *.rmk file import into RMK app.



RMK app configuration

Roger Mobile Key (RMK) app for Android and iOS systems can be downloaded and installed respectively from Google Play and App Store. After its installation, select ⋮ in the top right corner and then *Settings*. Enter the same encryption keys as in case of previous configuration of MCT terminals or leave empty if they were not defined in MCT



Encryption keys and Factor class will be applied only when credential is defined. Therefore it is possible to have credentials with different keys and class in the app, which can be then used on different MCT terminals.

More information on RMK app is given in its manual which is available at www.roger.pl.

Preliminary configuration of RACS 5

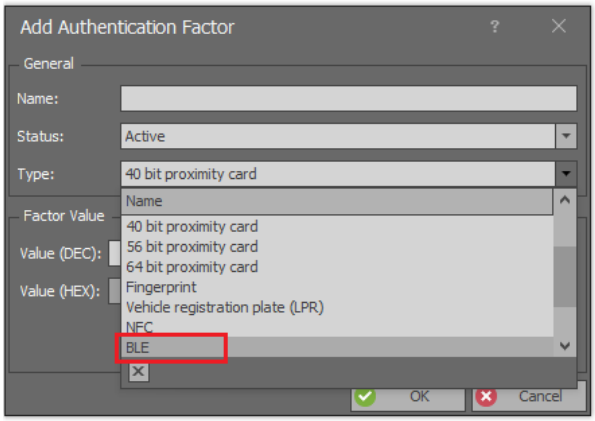
Configure the system in regard of low level configuration, database, services and high level configuration according to AN006 application note. The installation of recommended centralized database is explained in AN017 application note.

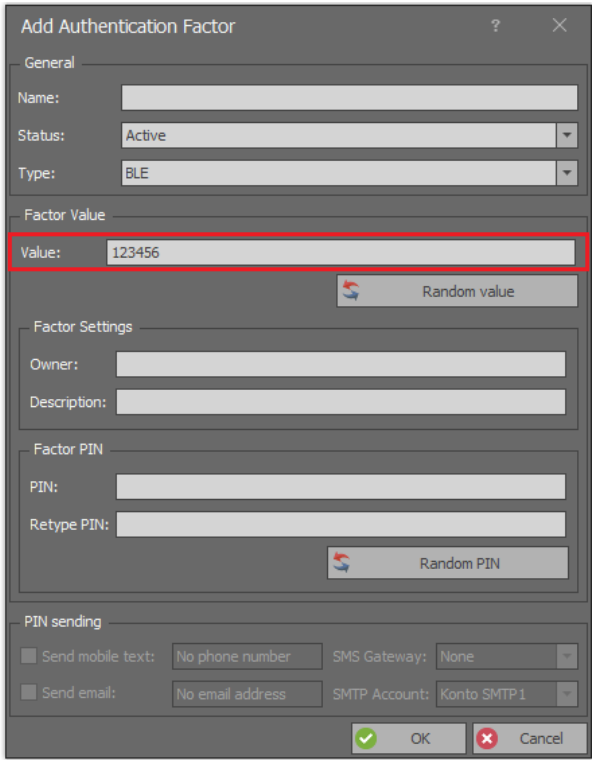
Mobile factors defining (method 1)

It is recommended to add and edit users as well as their Authentication Factors by means of wizards in VISO program. Authentication Factors can also be defined and sent on the level of Access Credential belonging to particular user.

In order to define Access User with BLE mobile Authentication Factor:

- In the top menu of VISO software select *Wizards* and then *Add Person online*
- Define Access Credential and assign Authorisations within the wizard according to AN006 application note.
- When Authentication Factor is defined then select *BLE* type.





- Enter value for the factor that will be used to recognize user during identification. This number is equivalent of proximity card number or PIN. The value 123456 is example. Close the window with *OK* button.
- Optionally define more Authentications Factors for the user. They can be various types including NFC type. The maximal number of Authentication Factors within Access Credential of particular Access User equals to 8.
- Proceed to the next steps of wizard, synchronise settings with MC16 controllers and close the wizard.
- Open RMK app on mobile device.
- In the top right corner select ⋮ and then *Add credential*.
- On the screen select *Bluetooth* (BLE), name the factor and then enter its value. According to previous settings it will be 123456. When the factor is created then encryption keys and class are applied according to settings in RMK app. They must be the same as in case of terminal where user will identify.

A user with NFC type Authentication Factor is defined in similar way.

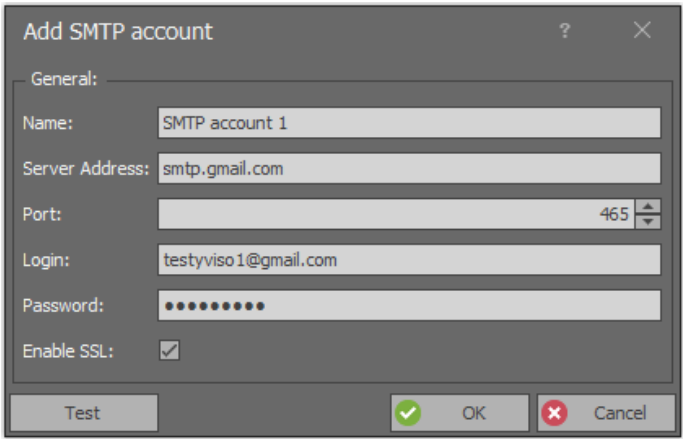
Mobile factors defining (method 2)

Mobile factors can be defined in VISO software and then sent as *.rmk files to user via email. Additionally such Authentication Factor can be secured with password (PIN) which can be sent to the user via email or mobile text.

SMTP server / SMS gate

In order to define SMTP server for email sending by VISO software:

- In the top menu of VISO software select *Tools* command and then *SMTP Accounts*. In the opened window select *Add* button.
- In the next window define parameters of SMTP account which can be used by RACS 5 system for e-mail sending (example below). Account settings can be verified with *Test* button. Close the window with *OK* button.

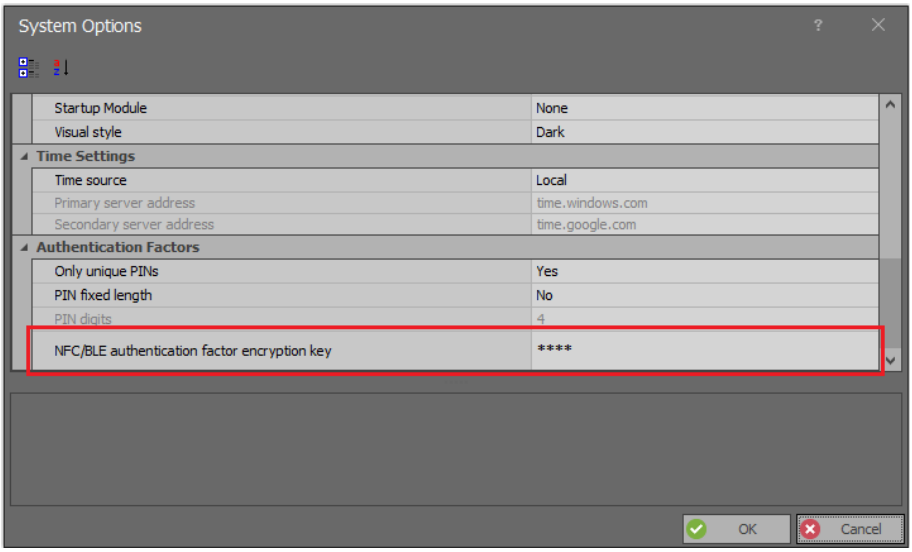


Similarly SMS Gate can be defined for mobile text sending by selection of *Tools* in the top menu of VISO software and then *SMS Gates*.

NFC/BLE authentication factor encryption key in VISO

If default empty NFC/BLE authentication factor encryption key was replaced in MCT terminal(s) with own one then it is necessary to enter this key in VISO software:

- In the top menu of VISO software select *Tools* command and then *System Options* icon.
- In the opened window enter the same encryption key as in MCT terminal(s). This key will be used when mobile factor is created and sent to user by email.

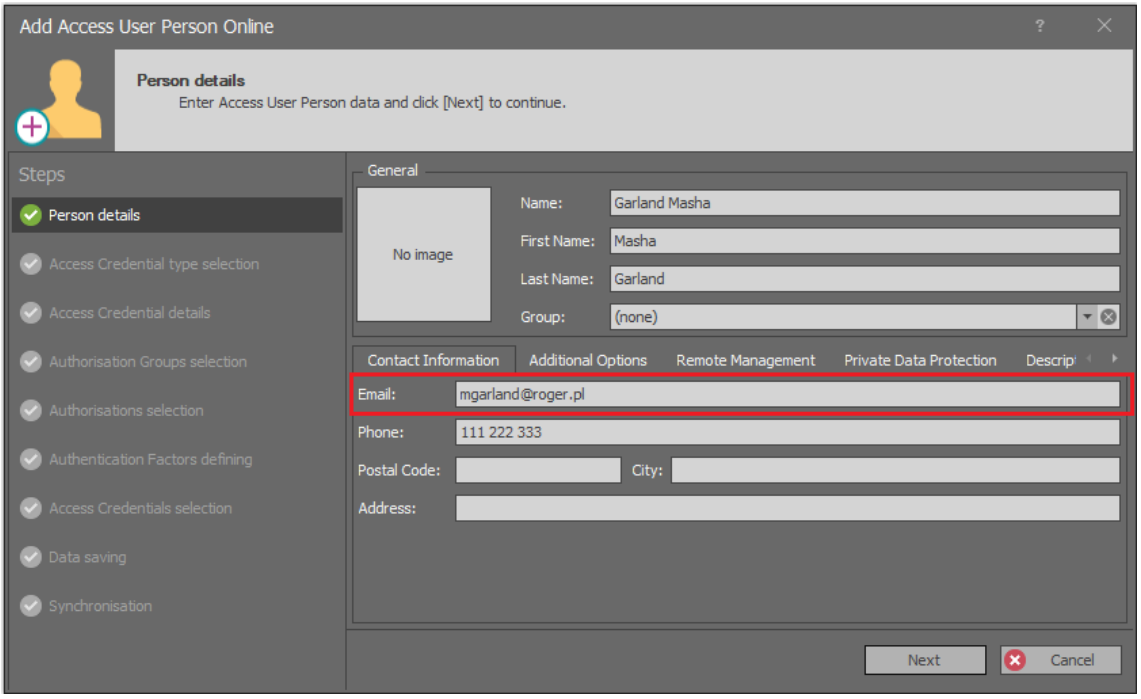


User and Authentication Factor defining

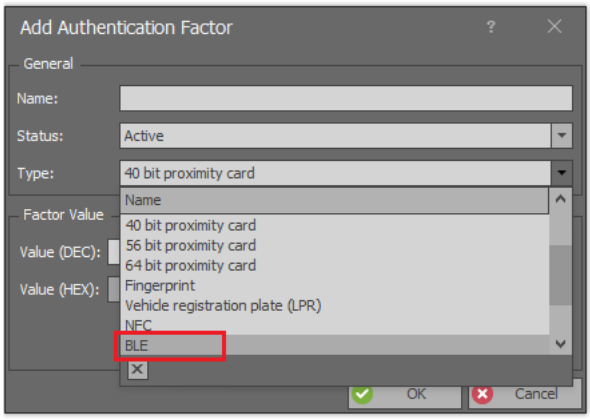
It is recommended to add and edit users as well as their Authentication Factors by means of wizards in VISO program. Authentication Factors can also be defined and sent on the level of Access Credential belonging to particular user.

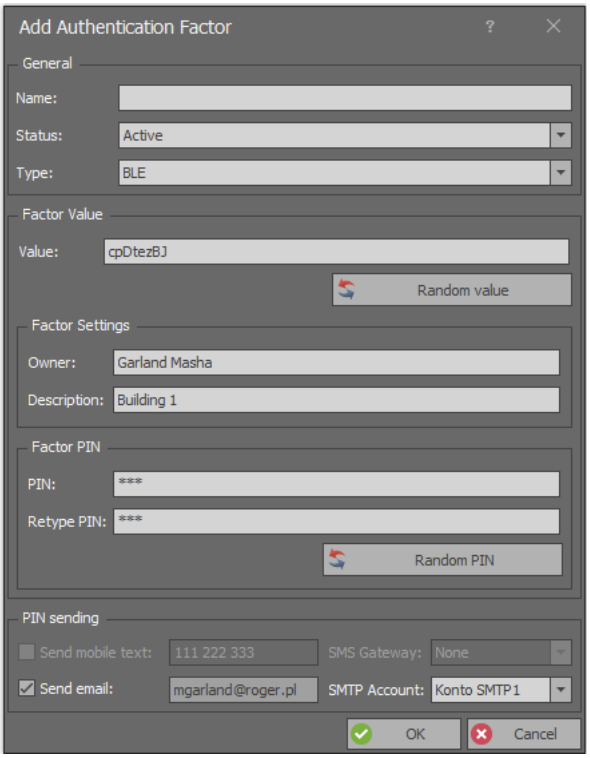
In order to define user and then send BLE type factor by email to this user:

- In the top menu of VISO software select *Wizards* and then *Add Person online*.
- In the opened window define not only first and last name but also email address for the user. This email will be used when Authentication Factors and/or passwords will be sent to the user. If mobile factor password (PIN) sending via mobile text is considered then additionally define mobile phone number for the user.



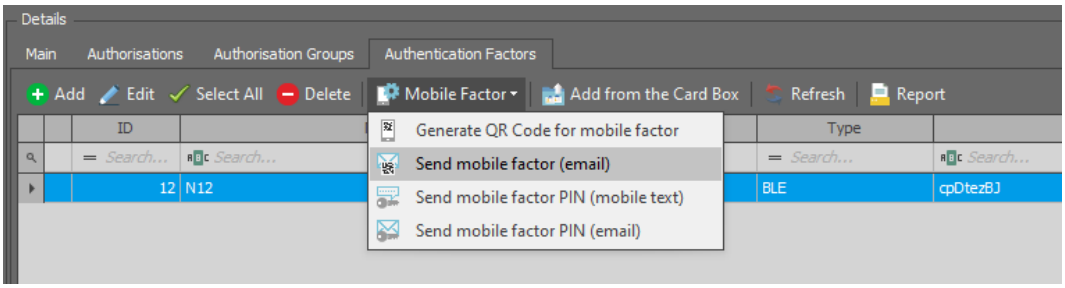
- Define Access Credential and assign Authorisations within the wizard according to AN006 application note.
- When Authentication Factor is defined then select *BLE* type.





- In the opened window enter own value or generate random one for the Authentication Factor. *Factor Settings* area is optional and it is used for description only. *Factor PIN* area is used to define optional password (PIN) for the Authentication Factor. When Authentication Factor is received by email then it can be imported to RMK app only if this password (PIN) is entered properly. In *PIN sending* area an email or mobile phone can be selected for automatic sending of the password (PIN) to the user. Close the window with *OK* button.

- Optionally define more Authentications Factors for the user. They can be various types including NFC type. The maximal number of Authentication Factors within Access Credential of particular Access User equals to 8.
- Proceed to the next steps of wizard, synchronise settings with MC16 controllers and close the wizard. If Authentication Factor password (PIN) is defined then it will be automatically sent to the user.
- In the top menu of VISO software select *Configuration* and then *Access Credentials*.
- Select Access Credential of just created Masha Garland user.
- In the bottom select *Authentication Factors* tab.
- Select previously created factor with value cpDtezBJ, then select *Mobile Factor* and *Send mobile factor (email)* command in order to send email to the user with *.rmk file attached. This file can be further imported in RMK app as credential.



- Open *.rmk file in RMK app on mobile device.
- In the opened window enter password (PIN) and previously defined NFC/BLE communication encryption key to import the file as credential for user identification. If the encryption key in MCT terminal(s) is default empty one then it is not necessary to enter it during file import.

A user with NFC type Authentication Factor is defined in similar way.

Note: Authentication Factor can not only be sent by email as *.rmk file. The alternative method is to generate QR code in VISO software. Such code can be displayed on screen, saved as pdf or printed and then it can be scanned in RMK app by selection of ⋮ and then *Add credential from QR code*.

Note: The class of credential imported from *.rmk file or QR code is REK.

Contact:
Roger sp. z o.o. sp.k.
82-400 Sztum
Gościszewo 59
Tel.: +48 55 272 0132
Fax: +48 55 272 0133
Tech. support: +48 55 267 0126
E-mail: support@roger.pl
Web: www.roger.pl