Roger Access Control System 5v2

Application note no. 046

Document version: Rev. A

Mobile identification and QR codes

Note: This document refers to RACS 5 v2.0.8 or higher and RMK app v3.x or higher

Introduction

Users can be identified in RACS 5 access control system not only by means of such typical Authentication Factors as proximity cards, PINs, fingerprints but also by mobile devices with installed RMK app (Android/iOS) and by barcodes including QR codes. The mobile identification can be in NFC (Near Field Communication) technology or BLE (Bluetooth Low Energy) technology at such terminals as MCT80M-BLE, MCT88M-IO and MCT84M-BK-QB which must be connected to MC16 access controller. The identification by means of QR codes and barcodes is possible using MCT84M-BK-QB terminal 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 user on MCT terminal by:
  - selection of credential in RMK app and then reading mobile device at the terminal (NFC/QR)
  - selection of credential in RMK app and then reading mobile device in distance of up to 10 meters from the terminal (BLE)
- Identify user on MCT terminals by QR code/barcode which can be displayed on mobile device or printed on paper.

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.

Preliminary configuration of RACS 5

Connect MCT terminals to MC16 access controllers and configure the system in regard of low level configuration, database, servers and high level configuration including Access Doors, Access Points and Authorisations according to AN006 and AN017 application notes.

Mobile identification

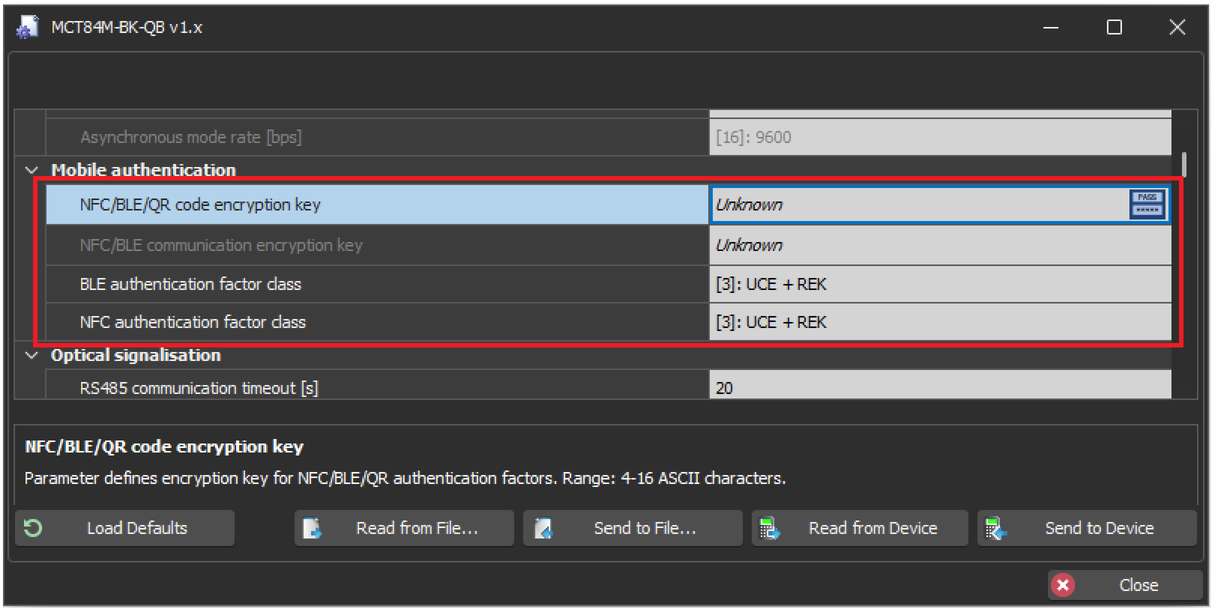
Mobile identification consists in using mobile device with RMK app installed to identify the user on the reader.

Terminal configuration

According to its installation manual, the low level configuration of a terminal for mobile identification can be made with VISO v2 when the terminal is connected to MC16 controller. Alternatively such configuration can be made with RogerVDM software and RUD-1 interface.

In case of mobile identification terminals except for typical addressing on RS485 bus it is possible to define own values for such parameters as *NFC/BLE/QR code encryption key* and *NFC/BLE communication encryption key* or default values can be left unchanged for these keys. Additionally factor class can be defined both for NFC and BLE. It is recommended to apply the option *[3]: UCE + REK* for both classes.

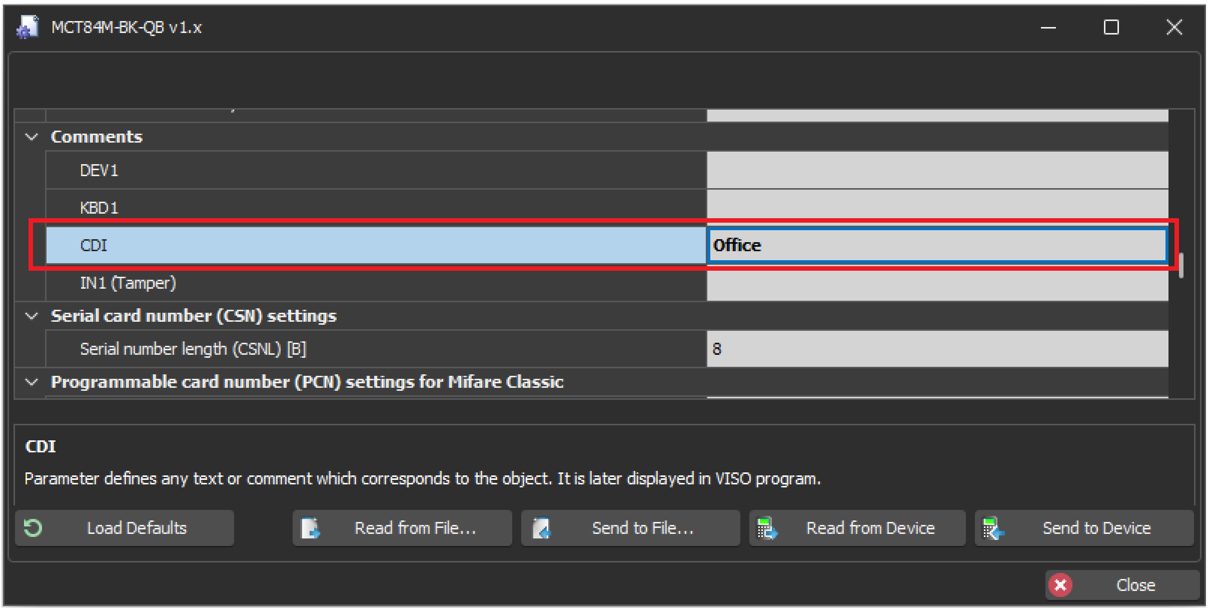
Note: *NFC/BLE/QR code encryption key* is irrelevant if further explained methods 1 and 2 are used to define mobile factors while in case of methods 2 and 3 it might be useful not to change default *NFC/BLE communication encryption key* in order to simplify rmk file and/or QR code import into RMK app.



Asynchronous mode rate [bps]	[16]: 9600
Mobile authentication	
NFC/BLE/QR code encryption key	*Unknown*
NFC/BLE communication encryption key	*Unknown*
BLE authentication factor class	[3]: UCE + REK
NFC authentication factor class	[3]: UCE + REK
Optical signalisation	
RS485 communication timeout [s]	20

NFC/BLE/QR code encryption key
Parameter defines encryption key for NFC/BLE/QR authentication factors. Range: 4-16 ASCII characters.

Additionally it is recommended to name CDI object of a MCT reader. This comment will be later displayed during user identification with RMK app and will facilitate the selection of adequate door to open when multiple BLE readers will be detected in a vicinity. This functionality requires at least firmware version 1.0.8.219 for MCT80M-BLE and MCT88M-IO terminals and at least firmware version 1.0.10.216 for MCT84M-BK-QB terminal.



Comments	
DEV1	
KBD1	
CDI	Office
IN1 (Tamper)	
Serial card number (CSN) settings	
Serial number length (CSNL) [B]	8
Programmable card number (PCN) settings for Mifare Classic	

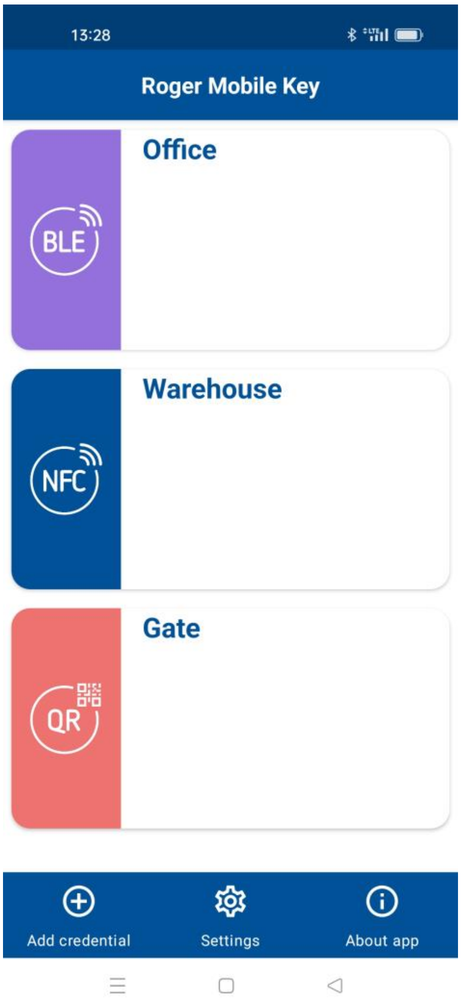
CDI
Parameter defines any text or comment which corresponds to the object. It is later displayed in VISO program.

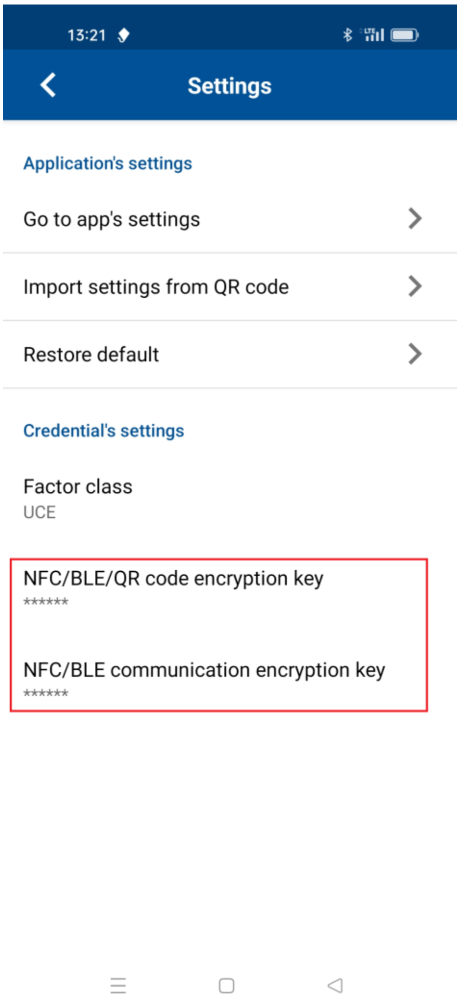
RMK app configuration

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

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

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





Factor class
UCE

NFC/BLE/QR code encryption key
******

NFC/BLE communication encryption key
******

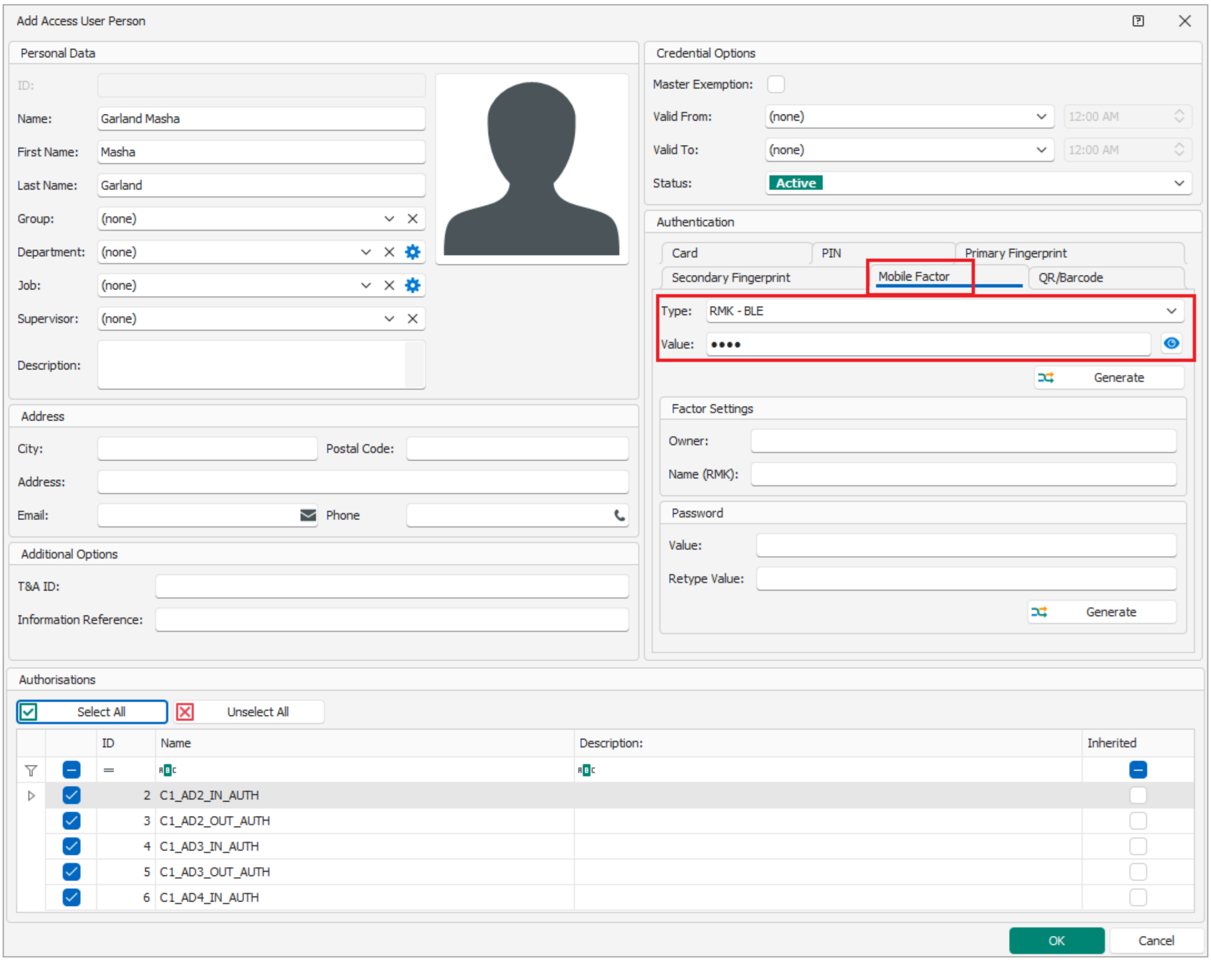
Mobile factor defining (method 1)

This method consists in defining of Authentication Factor in VISO software and then defining corresponding credential with the same parameters in RMK app.

It is recommended to use simple *Add Person Quickly* wizard for the purpose of Person and Authentication Factor(s) defining but more complex *Add Person Online* wizard can also be applied. The second one can be started by selection of *Wizards* in the top menu of VISO software. Authentication Factors can also be added, edited and uploaded on the level of Access Credentials belonging to Persons.

In order to define Person with BLE mobile Authentication Factor using *Add Person Quickly*:

- In the top menu of VISO software select *Configuration* and then *Access User Persons*
- In the opened window expand *Add* button and select *Add Person Quickly*.
- In the next window name the Person, select relevant Authorisations (access rights) and in *Mobile Factor* tab select *RMK-BLE*.
- Enter value for the factor that will be used to recognize user during identification at readers. This number is equivalent of proximity card number or PIN.
- Optionally define more Authentications Factors of other types.



Add Access User Person

Personal Data

ID:

Name: Garland Masha

First Name: Masha

Last Name: Garland

Group: (none)

Department: (none)

Job: (none)

Supervisor: (none)

Description:

Address

City:

Postal Code:

Address:

Email:

Phone

Additional Options

T&A ID:

Information Reference:

Credential Options

Master Exemption: □

Valid From: (none) 12:00 AM

Valid To: (none) 12:00 AM

Status: Active

Authentication

Type: RMK - BLE

Value: ••••

Factor Settings

Owner:

Name (RMK):

Password

Value:

Retype Value:

Authorisations

	ID	Name	Description:	Inherited
☑	2	C1_AD2_IN_AUTH		□
☑	3	C1_AD2_OUT_AUTH		□
☑	4	C1_AD3_IN_AUTH		□
☑	5	C1_AD3_OUT_AUTH		□
☑	6	C1_AD4_IN_AUTH		□

- Close the window with *OK* button and then select *No* in order to reject additional steps related to the mobile factor.
- Select *Synchronise* button in order to upload the Person to the system.
- Open RMK app on mobile device and select *Add credential*.
- On the screen select *Bluetooth* (BLE), name the factor and then enter the same value as previously in VISO software. 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 factor defining – QR code (method 2)

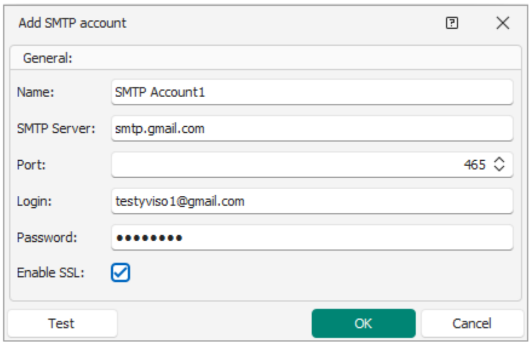
This method is similar to method 1 and the difference is such that credential is added in RMK app not by entering its value but by QR code scanning. Such credential can include its name, be protected with password and paired with MCT readers. Such pairing can facilitate user identification as it will not be necessary to manually select MCT reader after selection of credential in RMK app. Therefore access granting can be easier and faster and it practical applications it is often applied on frequently accessed doors e.g. main door to a building.

SMTP server / SMS gate

It is optional to define SMTP server and/or SMS gate and it is required only if password is defined for mobile factor and then it is necessary to send it to user by email or mobile text (SMS).

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.

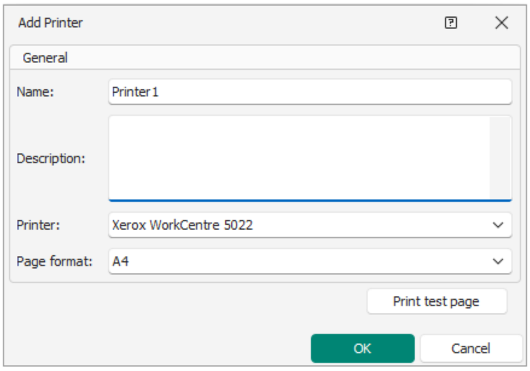

Add SMTP account
General:
Name: SMTP Account1
SMTP Server: smtp.gmail.com
Port: 465
Login: testyviso1@gmail.com
Password: ••••••••
Enable SSL: ☑

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*. Additionally it will be necessary to register an account at smsapi.pl.

Printer

It is optional to define printer and it is required only if QR codes are supposed to be printed on paper. In order to define a printer:

- In the top menu of VISO software select *Tools* command and then *Printers*. In the opened window select *Add* button.
- In the next window select a printer previously installed on the computer.

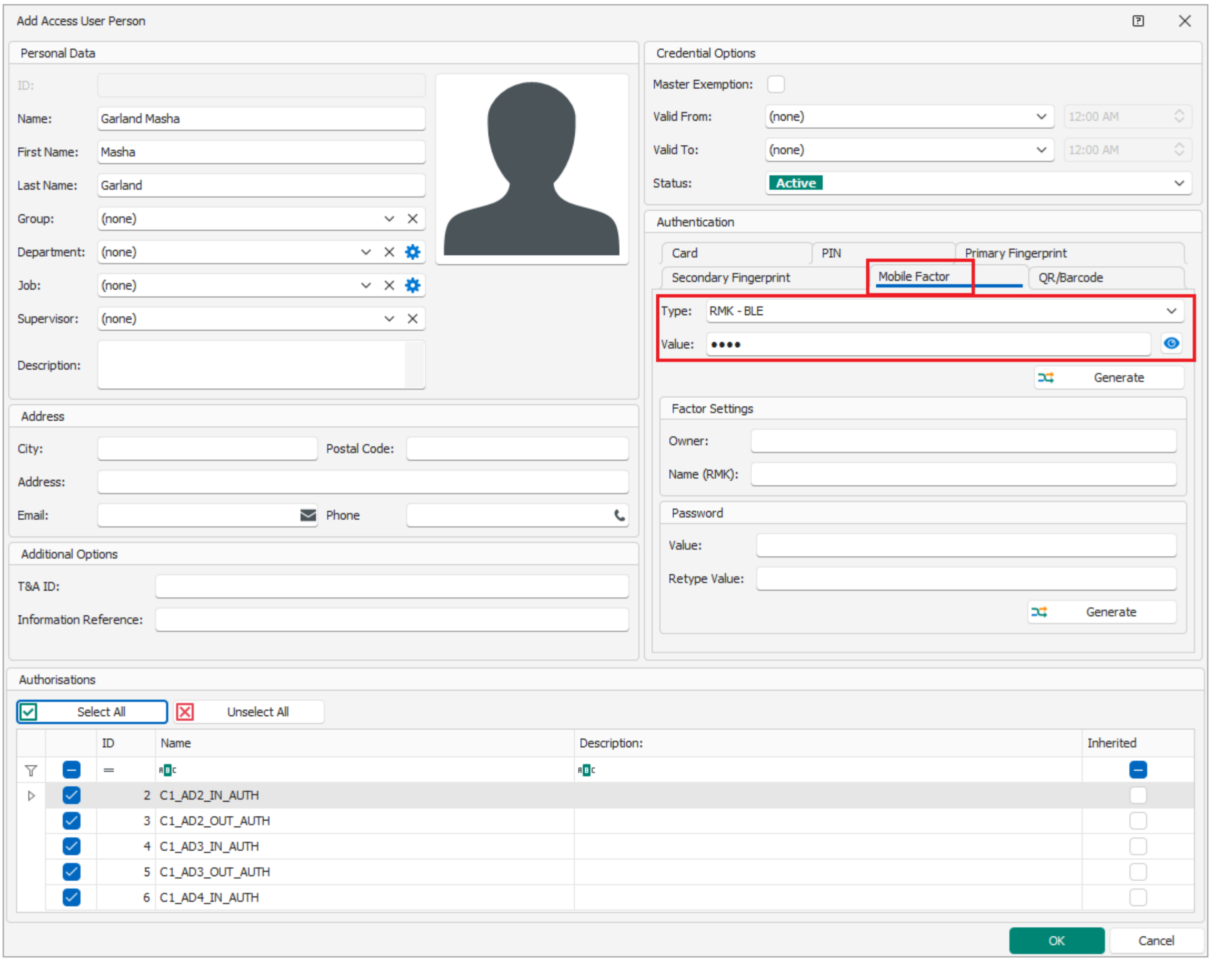

Add Printer
General
Name: Printer1
Description:
Printer: Xerox WorkCentre 5022
Page format: A4

Person and Authentication Factor defining

In order to define Person with BLE mobile Authentication Factor using *Add Person Quickly*:

- In the top menu of VISO software select *Configuration* and then *Access User Persons*
- In the opened window expand *Add* button and select *Add Person Quickly*.
- In the next window name the Person, select relevant Authorisations (access rights) and in *Mobile Factor* tab select *RMK-BLE*. Define email address and/or phone number if mobile factor password is supposed to be defined for the factor.

- Enter value for the factor that will be used to recognize user during identification at readers. This number is equivalent of proximity card number or PIN. Optionally enter name of the factor in *Name (RMK)* so it will be displayed in RMK app and optionally define password for the factor
- Optionally define more Authentications Factors of other types.



Add Access User Person

Personal Data

ID:
Name: Garland Masha
First Name: Masha
Last Name: Garland
Group: (none)
Department: (none)
Job: (none)
Supervisor: (none)
Description:

Address

City:
Postal Code:
Address:
Email:
Phone

Additional Options

T&A ID:
Information Reference:

Credential Options

Master Exemption: □
Valid From: (none) 12:00 AM
Valid To: (none) 12:00 AM
Status: Active

Authentication

Card | PIN | Primary Fingerprint | Secondary Fingerprint | Mobile Factor | QR/Barcode

Type: RMK - BLE
Value: ••••
Generate

Factor Settings

Owner:
Name (RMK):

Password

Value:
Retype Value:
Generate

Authorisations

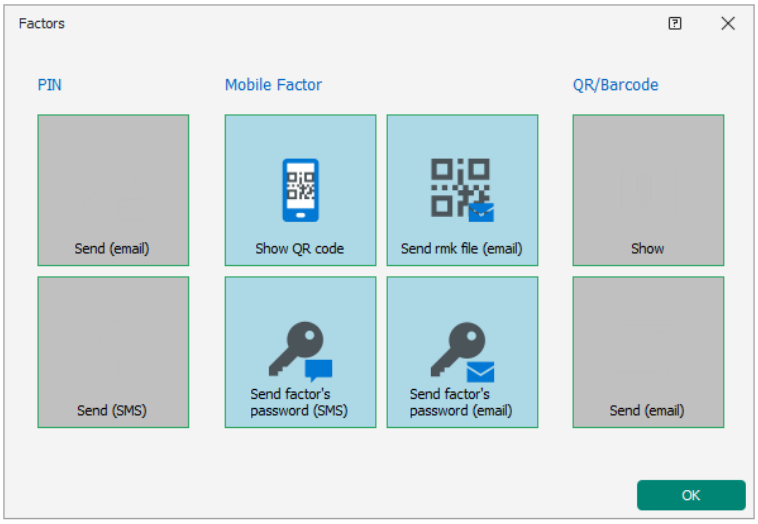
☑ Select All ☒ Unselect All

	ID	Name	Description:	Inherited
☑	2	C1_AD2_IN_AUTH		□
☑	3	C1_AD2_OUT_AUTH		□
☑	4	C1_AD3_IN_AUTH		□
☑	5	C1_AD3_OUT_AUTH		□
☑	6	C1_AD4_IN_AUTH		□

OK Cancel

- Close the window with *OK* button and then select *Yes* in order to proceed with additional steps related to mobile factor.
- In the opened window select *Show QR code* and in the next window save the code as PDF or print the code. Make this QR code available to the user with RMK app. If password is defined for the mobile factor then it can be send to user via email or mobile text (SMS) as it will be later needed when mobile factor is imported in RMK app.

Note: Additional steps related to mobile factor can also be taken later for particular Persons by selecting *Access Credentials* tab in the bottom, then clicking particular Access Credential and in the opened window selecting *Authentication Factors* tab where *Mobile Factor* button is available. Alternatively select *Configuration* in the top menu of VISO software, then *Access Credentials* and for particular Access Credential of a Person in the bottom select *Authentication Factors* tab where *Mobile Factor* button is available.



- Open RMK app on mobile device and select *Add credential*.
- On the screen select *ADD CREDENTIAL FROM QR CODE* and then scan QR code which was previously generated in VISO software. Enter password if applicable. The name of factor will be filled if it was defined in VISO software. 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 factor defining – rmk file (method 3)

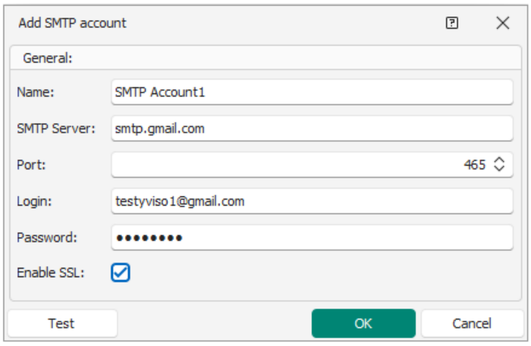
This method is similar to method 2 and the difference is such that credential is added in RMK app not by QR code scanning but by rmk file importing. Such credential can include its name, be protected with password and paired with MCT readers. Such pairing can facilitate user identification as it will not be necessary to manually select MCT reader after selection of credential in RMK app. Therefore access granting can be easier and faster and it practical applications it is often applied on frequently accessed doors e.g. main door to a building.

SMTP server / SMS gate

It is recommended to define SMTP server and/or SMS gate as they are required to send factor's password to user by email or mobile text (SMS). Additionally rmk file can also be send from VISO program to user by email.

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.



Add SMTP account

General:

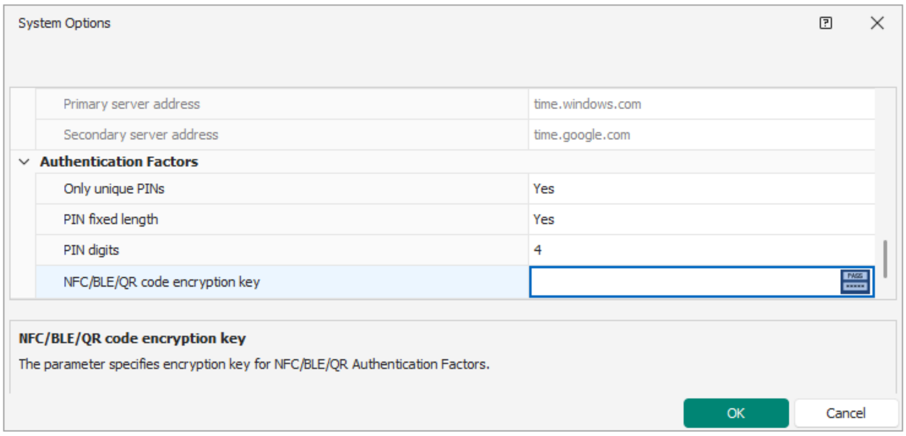
Name:	SMTP Account1
SMTP Server:	smtp.gmail.com
Port:	465
Login:	testyviso1@gmail.com
Password:	••••••••
Enable SSL:	☑

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*. Additionally it will be necessary to register an account at smsapi.pl.

NFC/BLE code encryption key in VISO

If default empty NFC/BLE code 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.



System Options

Primary server address	time.windows.com
Secondary server address	time.google.com
Authentication Factors	
Only unique PINs	Yes
PIN fixed length	Yes
PIN digits	4
NFC/BLE/QR code encryption key	

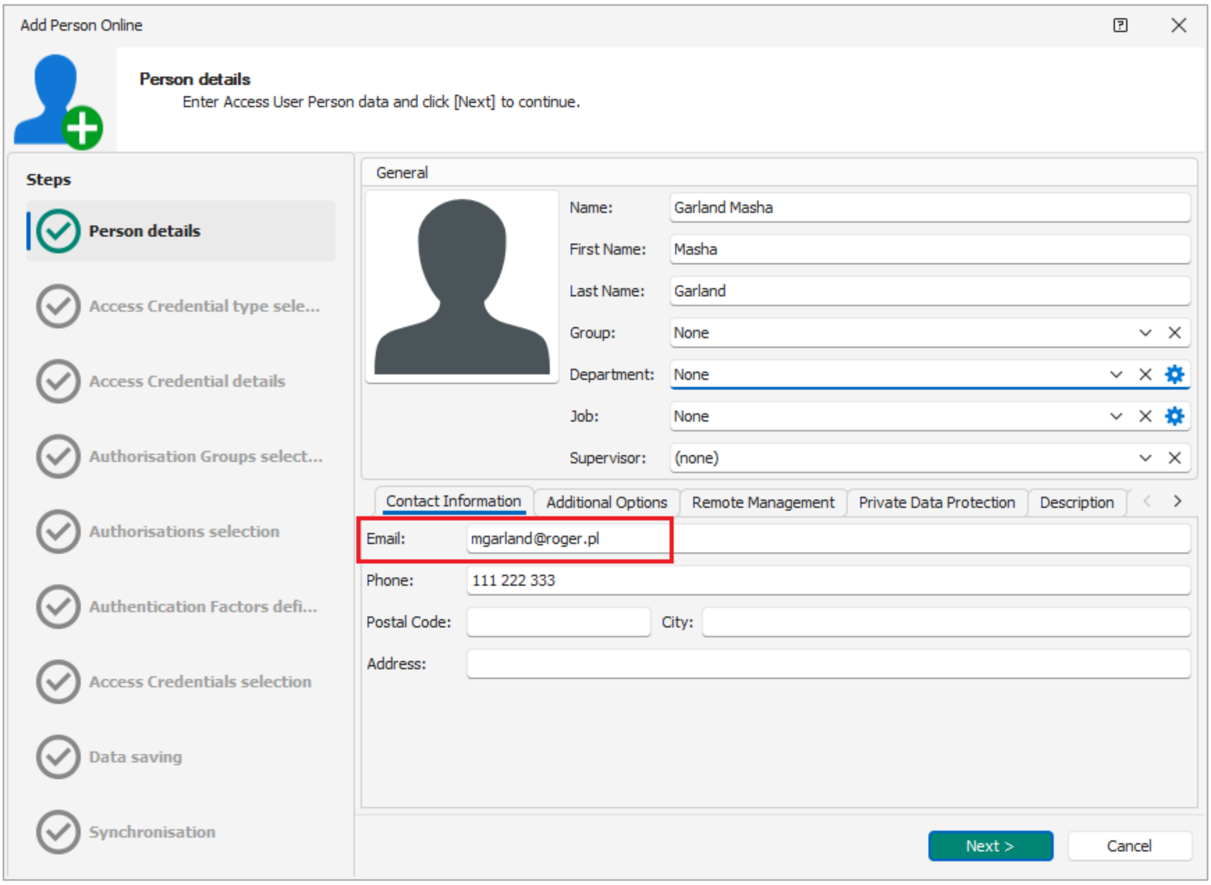
NFC/BLE/QR code encryption key

The parameter specifies encryption key for NFC/BLE/QR Authentication Factors.

Person and Authentication Factor defining

In order to define Person with BLE mobile Authentication Factor using *Add Person Online*:

- 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 various Authentication Factors and/or passwords will be sent to the user. If mobile factor password sending via mobile text (SMS) is considered then additionally define mobile phone number for the user.



Add Person Online

Person details

Enter Access User Person data and click [Next] to continue.

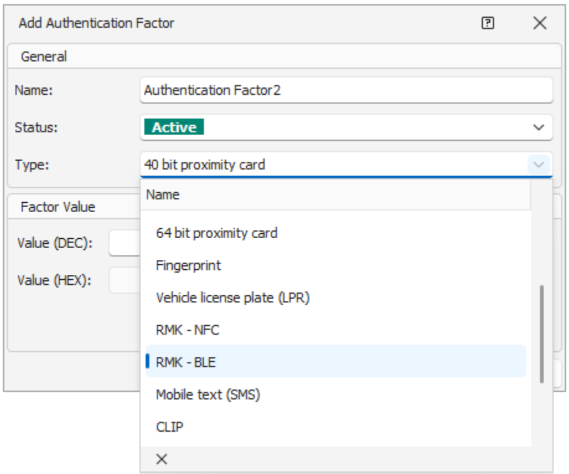
Steps
- Person details
- Access Credential type sele...
- Access Credential details
- Authorisation Groups select...
- Authorisations selection
- Authentication Factors defi...
- Access Credentials selection
- Data saving
- Synchronisation

General

Name:	Garland Masha
First Name:	Masha
Last Name:	Garland
Group:	None
Department:	None
Job:	None
Supervisor:	(none)

Email:	mgarland@roger.pl
Phone:	111 222 333
Postal Code:	
City:	
Address:	

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



Add Authentication Factor

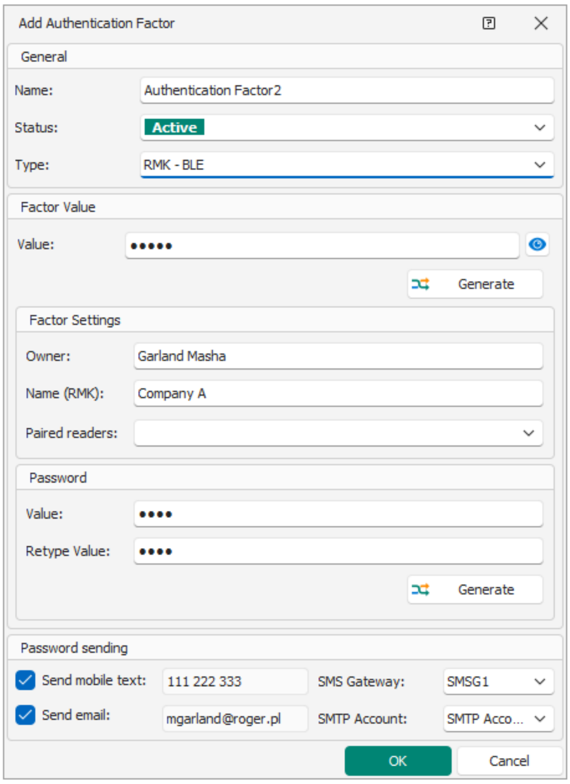
General

Name:	Authentication Factor2
Status:	Active
Type:	40 bit proximity card

Factor Value

Value (DEC):

Value (HEX):



Add Authentication Factor

General

Name:	Authentication Factor2
Status:	Active
Type:	RMK - BLE

Factor Value

Value: •••••

Factor Settings

Owner:	Garland Masha
Name (RMK):	Company A
Paired readers:	

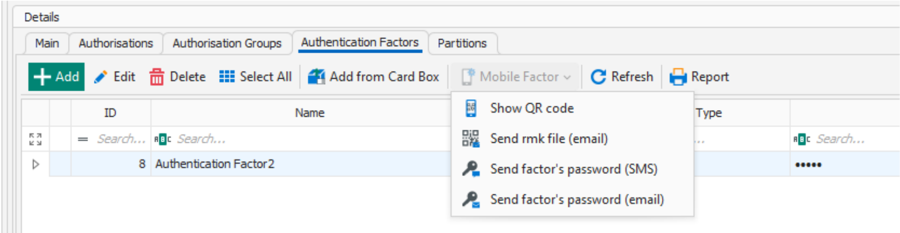
Password

Value:	••••
Retype Value:	••••

Password sending

☑ Send mobile text:	111 222 333	SMS Gateway:	SMSG1
☑ Send email:	mgarland@roger.pl	SMTP Account:	SMTP Acco...

- Enter value for the factor or generate random value. In the *Name (RMK)* field define the name of Authenticator Factor to be displayed in RMK app. Additionally, Access Points (MCT readers) can be paired with the factor. Optional password can be defined in order to secure the importing of factor in RMK app. It is possible to select the method for password sending and to select relevant SMTP server and/or SMS gate.
- 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 password is defined then it will be sent automatically by wizard.
- In the top menu of VISO software select *Configuration* and then *Access Credentials*.
- Select Access Credential belonging to Masha Garland user from the list.
- Select *Authentication Factors* tab in the bottom.
- Select previously created BLE Authentication Factor, expand *Mobile Factor* and select *Send rmk file (email)* so the factor could be sent to the email address of Masha Garland user.



- On mobile device with RMK app open received email and click attached rmk file in order to import it into RMK app.
- If both factor's password and NFC/BLE/QR communication password are defined then enter them during import. If not then leave them empty.

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

Note: The class of imported credential is REK.

QR codes and barcodes identification

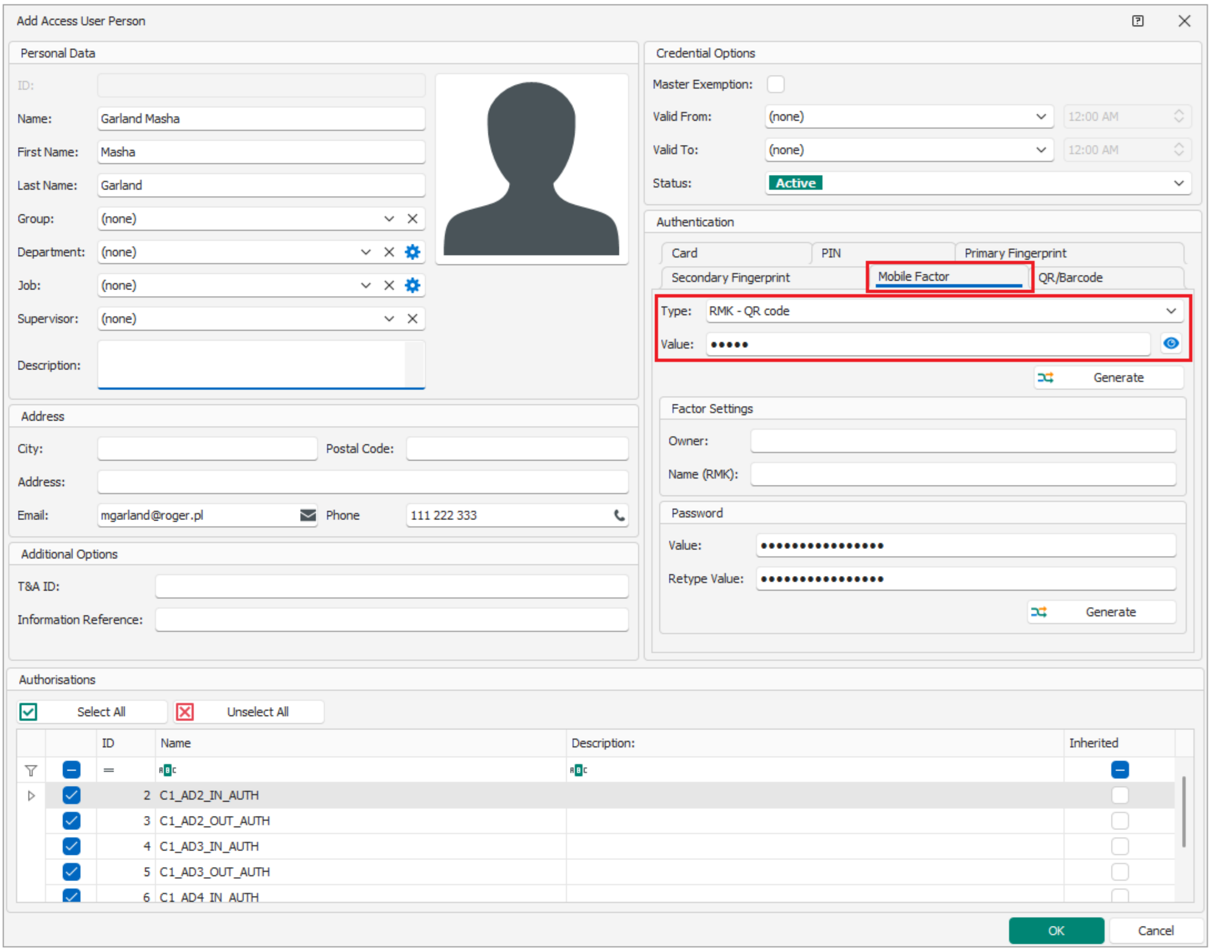
QR/barcode identification involves the use of a code that can be printed on a piece of paper or displayed on the screen of a mobile device and then read on the MCT84M-BK-QB terminal to identify the user. Following codes can be used in the system:

- Encrypted QR codes for RMK app
- Plain QR codes
- Barcodes

Encrypted QR codes (RMK app)

Encrypted QR codes belong to the same class as the previously described BLE and NFC mobile factors. They can only be defined in the VISO software and the RMK application because the algorithm for their generation and encryption is confidential. Encrypted QR codes are usually used within the RMK application, but they can also be displayed in VISO and saved as a PDF document for possible sending to the user.

Similarly to other mobile factors, it is possible to define your own value or use the default value for the *NFC/BLE/QR code encryption key* parameter within low level configuration of the MCT84M-BK-QB reader as well as in the RMK app and in the VISO software. Mobile factors of *RMK - QR Code* type can be defined with method 1, i.e. by manually adding them in the VISO program and the RMK app, and with method 3 using the *Add Person Online* wizard and sending the rmk file by email. Both methods are described in detail in the previous sections of the note. The difference is that when defining the factor, the type *RMK - QR code* is selected instead of *RMK - BLE*.



Add Access User Person

Personal Data

ID:	
Name:	Garland Masha
First Name:	Masha
Last Name:	Garland
Group:	(none)
Department:	(none)
Job:	(none)
Supervisor:	(none)
Description:	

Address

City:		Postal Code:	
Address:			
Email:	mgarland@roger.pl	Phone	111 222 333

Additional Options

T&A ID:	
Information Reference:	

Credential Options

Master Exemption:	□	
Valid From:	(none)	12:00 AM
Valid To:	(none)	12:00 AM
Status:	Active	

Authentication

Card | PIN | Primary Fingerprint | Secondary Fingerprint | Mobile Factor | QR/Barcode

Type:	RMK - QR code
Value:	●●●●●

Generate

Factor Settings

Owner:	
Name (RMK):	

Password

Value:	●●●●●●●●●●●●●●●●
Retype Value:	●●●●●●●●●●●●●●●●

Generate

Authorisations

☑ Select All ☒ Unselect All

		ID	Name	Description:	Inherited
	☑	2	C1_AD2_IN_AUTH		□
	☑	3	C1_AD2_OUT_AUTH		□
	☑	4	C1_AD3_IN_AUTH		□
	☑	5	C1_AD3_OUT_AUTH		□
	☑	6	C1_AD4_IN_AUTH		□

OK Cancel

Plain QR codes and barcodes

Commonly used plain unencrypted QR codes and barcodes can be also applied in RACS 5 system. They are generated in accordance with widely known algorithms. Therefore they can be created both in VISO software and by means of all kinds of publicly available generators. In such scenario of operation the RMK app is not used.

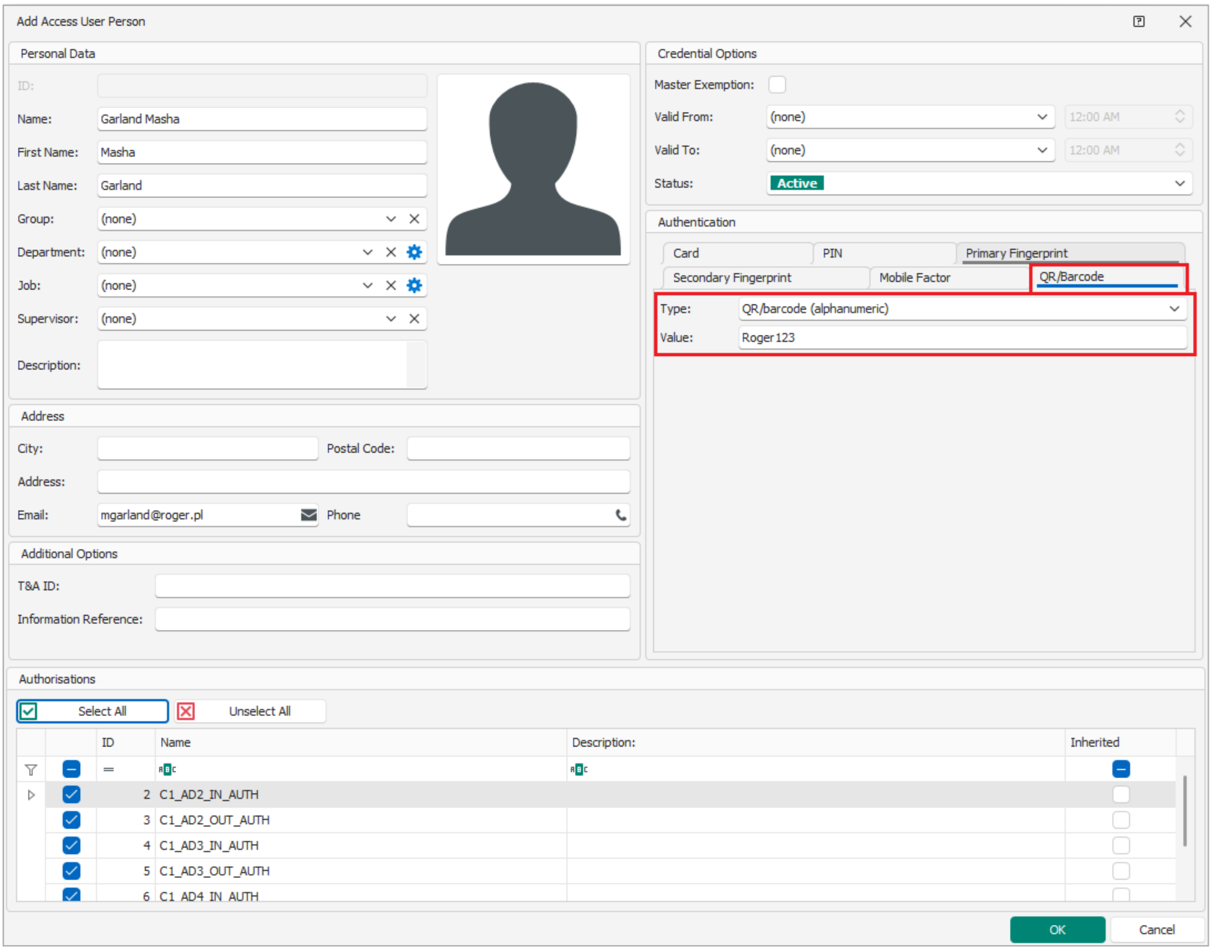
Terminal configuration

According to its installation manual, the low level configuration of MCT84M-BK-QB terminal can be made with VISO v2 when the terminal is connected to MC16 controller. Alternatively such configuration can be made with RogerVDM software and RUD-1 interface.

In case of such plain QR codes and barcodes it is necessary to modify the parameter *Format* in the section *Plain barcodes*. It is recommended to select the option *ASCII*.

Factor defining

QR codes and/or barcodes can be defined for a Person by means of wizards which are explained in previous sections using method 1 – *Add Person Quickly* wizard or method 3 – *Add Person Online* wizard. In such case *QR Code/barcode (alphanumeric)* type of Authentication Factor should be selected. Such Factor can include max. 8 visible ASCII characters i.e. from 0x20 to 0x7E excluding / (0x2F) and : (0x3A).



Add Access User Person

Personal Data

ID:
Name: Garland Masha
First Name: Masha
Last Name: Garland
Group: (none)
Department: (none)
Job: (none)
Supervisor: (none)
Description:

Address

City:
Postal Code:
Address:
Email: mgarland@roger.pl
Phone

Additional Options

T&A ID:
Information Reference:

Credential Options

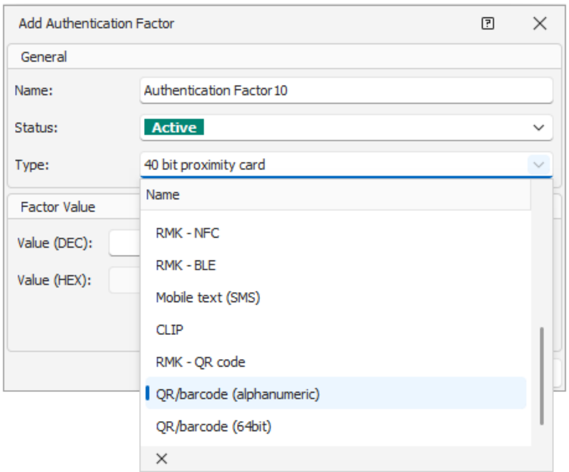
Master Exemption: □
Valid From: (none) 12:00 AM
Valid To: (none) 12:00 AM
Status: Active

Authentication

Type: QR/barcode (alphanumeric)
Value: Roger 123

Authorisations

	ID	Name	Description:	Inherited
☑	2	C1_AD2_IN_AUTH		□
☑	3	C1_AD2_OUT_AUTH		□
☑	4	C1_AD3_IN_AUTH		□
☑	5	C1_AD3_OUT_AUTH		□
☑	6	C1_AD4_IN_AUTH		□



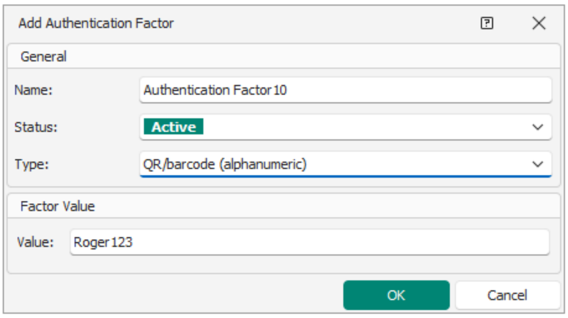
Add Authentication Factor

General

Name: Authentication Factor 10
Status: Active
Type: 40 bit proximity card

Factor Value

Value (DEC):
Value (HEX):



Add Authentication Factor

General

Name: Authentication Factor 10
Status: Active
Type: QR/barcode (alphanumeric)

Factor Value

Value: Roger 123

In both cases it is possible to display the code for entered value and sending the code via email to particular Person. SMTP server can be defined according to description in previous sections.

QR codes from third party software

Plain QR codes and/or barcodes can be generated by third party software and corresponding values can be uploaded to RACS 5 system via its API. As explained before, in such scenario it is necessary to make low level configuration of MCT84M-BK-QB terminal(s) in regard of the parameter *Format* in the section *Plain barcodes*. Depending on selected format:

- *ASCII* – the code can include max. 8 visible ASCII characters i.e. from 0x20 to 0x7E. Additionally it must be taken into consideration that / (0x2F) is changed by terminal into \ (0x5C) and : (0x3A) is changed by terminal into . (0x2E).

Example:

QR code	Auth. Factor type (VISO)	Factor value (VISO)
 Roger123	[16] QR/barcode (alphanumeric)	Roger123

- *HEX* – code can include max. 16 HEX characters i.e. 0-9 and A-F. Leading spaces and/or zeros are omitted by terminal.

QR code	Auth. Factor type (VISO)	Factor value (VISO)
 1234567890ABCDEF	[17] QR/barcode (64bit)	1311768467294899695 [DEC]

Note: In the low level configuration of the terminal the parameter *Maximal number of bytes* is by default set to 8. If codes are supposed to include 16 characters then it is necessary to modify the value into 16 bytes.

- *BIN* – the code can include max. 8 visible ASCII characters i.e. from 0x20 to 0x7E. Characters are modified by terminal into decimal number which corresponds to ASCII HEX characters.

QR code	Auth. Factor type (VISO)	Factor value (VISO)
 12345678	[17] QR/barcode (64bit)	3544952156018063160 [DEC] 31 32 33 34 35 36 37 38 [ASCII HEX]

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