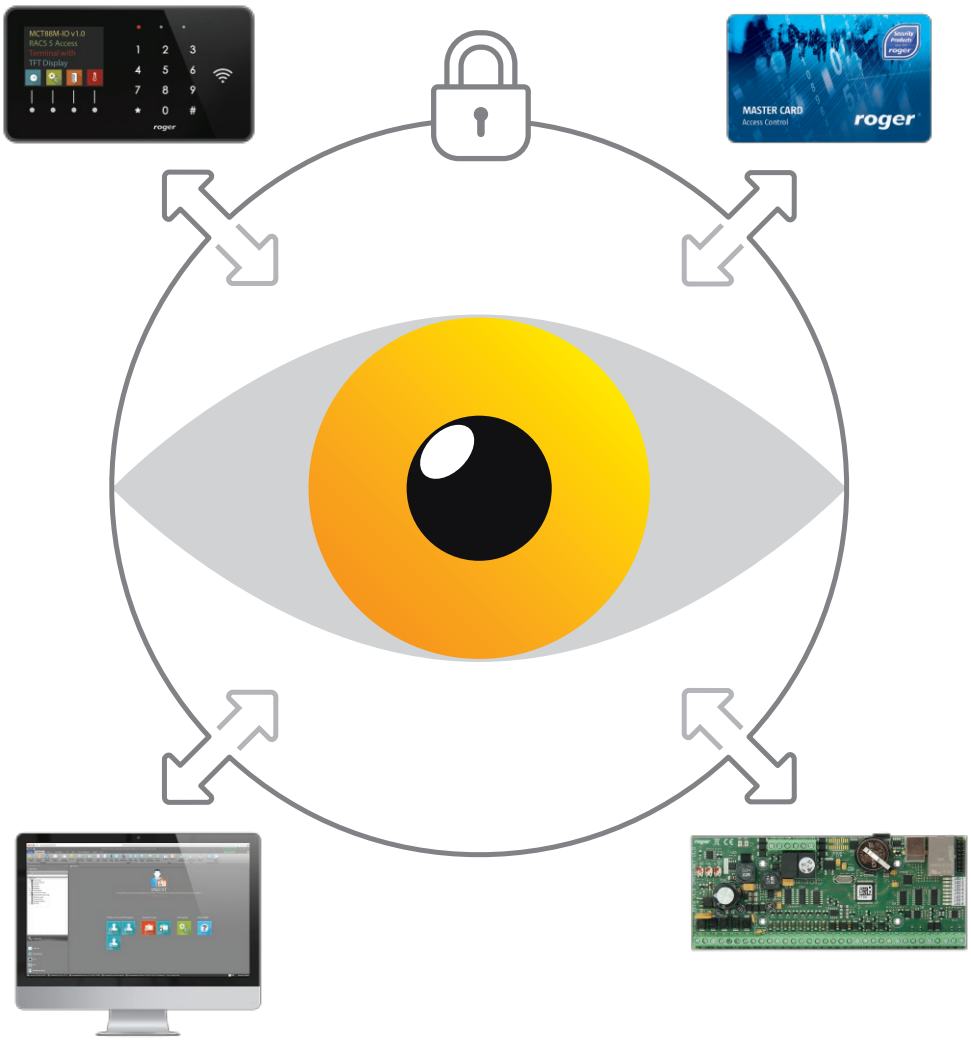
Security in RACS 5 Access Control System

- Database Encryption
- Encrypted Communication between Software and Devices
- Multilevel Access in RACS 5 Management Software and Operator Authentication
- Encrypted Proximity Card Numbers
- Biometric Identification of Users
- Multistage Identification of Users



roger®
Intelligence for Building

Security in RACS 5 Access Control System

RACS 5 system offers multi-layered security in order to prevent bypass of movement rules by users and asset in the area covered by the system. The security of system consists of three main elements: the use of identifiers secured against duplication, encryption of all types of communication used in the system, controlled access to its management software.

The RACS 5 system offers a large group of MCTxxM series readers that support MIFARE® proximity cards, including DESFire and Plus cards offering the highest level of encryption security. The MIFARE® card code can be stored in the encrypted sectors of its memory, so it is not possible to read it and thus duplicate it, even in the case of physical access to the card. Both the password encrypting the card code and its location in the MIFARE® card memory are subject to individual programming, which means that cards from other systems do not work in a given access control installation. Optionally, MIFARE® cards can be configured so that they can be used in many applications (systems) however, as long as the card codes are stored in separate data sector and secured with passwords, the security level of access control system is not reduced.

RACS 5 offers the possibility to identify users with their mobile devices. In such case the communication between the mobile device and RACS 5 terminal is encrypted and its interception does not pose a threat to security.

Another available security measure consists in multi-stage user authentication modes that require the use of more than one form of identification. The system offers both typical built-in identification modes such as "Card + PIN" and "Card + Fingerprint", and also enables configuration of your own complex modes e.g. "Card + PIN + Fingerprints". The RACS 5 system includes RFT1000 fingerprint reader, which can store fingerprint templates in its memory or can use templates stored in the memory of MIFARE® cards.

The use of MIFARE® proximity cards in combination with multi-stage authentication modes creates a very high security barrier, which can be additionally strengthened by the "Access by remote authorization" function and the "Two user entry" function. The first one makes access granting dependent on operator acceptance who can use CCTV cameras to visually identify a user prior to remote access granting. In case of the other function, access can be granted only after identification of two authorized users.

Communication between the system's management software (VISO) and access controllers is carried out via a computer network (LAN) and is encrypted using the AES128 CBC method. This method consists in encrypting communication by means of a dynamically changing password, which makes transmitted frames indecipherable and at the same prevents their replication. Internal communication between the access controller and readers and/or other modules can be provided with RS485 bus, computer network and wirelessly. In each of these cases it is encrypted and similarly to LAN communication with controller it is protected against replication.

Access to management software (VISO) requires authentication with password. The system can be operated by many operators with different authorization levels. Operator actions are recorded in a dedicated event log. This can be very useful when it is required to reconstruct course of events related to the management, configuration and operation of the system.

Note!
Contrary to standard MIFARE® card readers commonly offered in the market, PRTxxMF and MCTxxM (Roger) series readers enable operation with unencrypted (CSN) and encrypted (SSN) card numbers. If user identification in the access control system is based on EM 125 kHz or MIFARE® (CSN) cards then there is a risk of card cloning which is a very critical decrease in its security level. In systems where card cloning is a significant threat, readers with an encrypted card code (SSN) should be used (e.g. MCTxxM Roger series readers).

Features:
- Encrypted computer network communication
- Encrypted RS485 bus communication
- Encrypted wireless communication
- Encrypted database
- Encrypted NFC communication
- Encrypted Bluetooth communication
- Encrypted firmware of access controllers
- Support for encrypted card numbers (MIFARE® SSN)
- Biometric identification with fingerprints
- Multi-stage authentication modes for users
- Remote access authorization
- Two users entry mode
- System management software protected with login and password
- Configurable access levels for operators of system management software
- Operator actions registered in dedicated log

ROGER sp. z o.o. sp. k.
82-400 Sztum
Gościszewo 59
Poland

T. +48 55 272 0132
F. +48 55 272 0133
E. roger@roger.pl
www.roger.pl