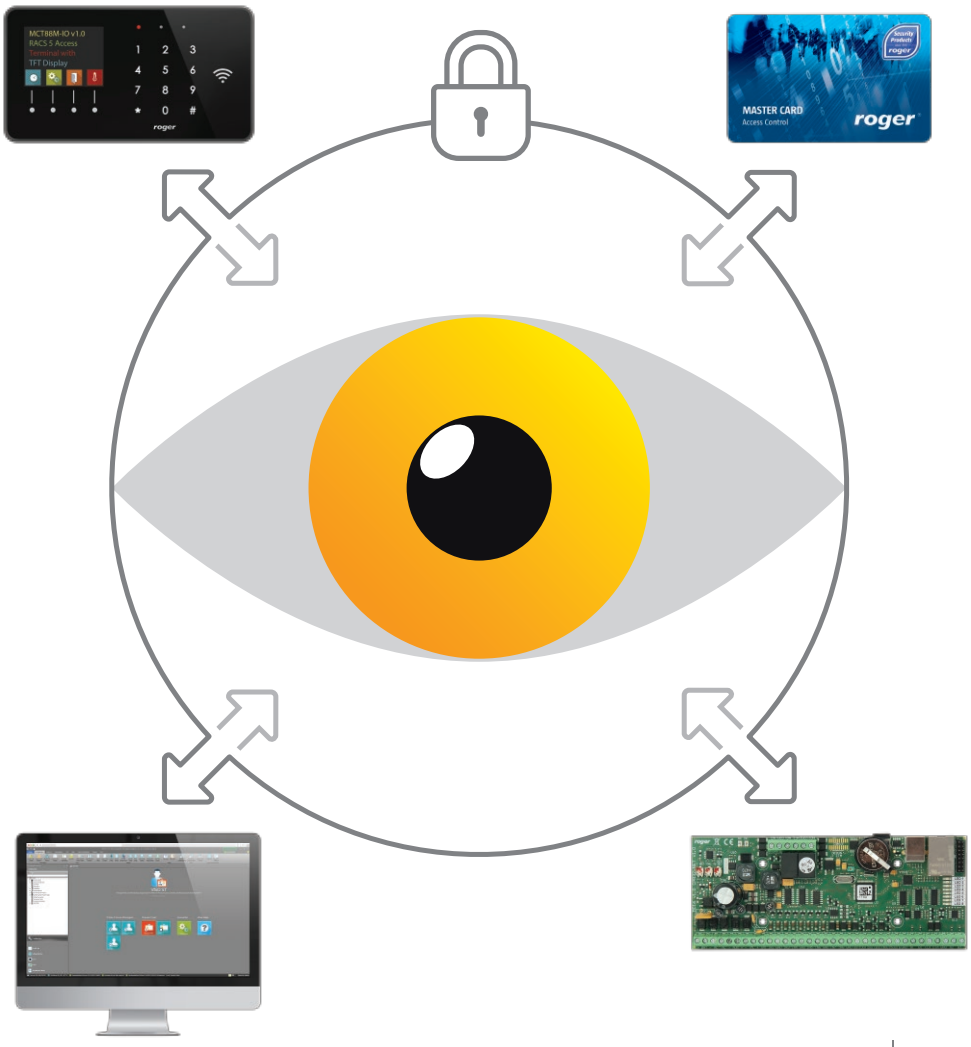
Zabezpieczenia w systemie kontroli dostępu RACS 5

- Szyfrowana baza danych
- Szyfrowana komunikacja między urządzeniami i oprogramowaniem
- Wielopoziomowy dostęp do oprogramowania z autoryzacją operatorów
- Szyfrowanie danych na karcie
- Biometryczne metody identyfikacji użytkowników
- Wieloetapowe tryby identyfikacji użytkowników



roger®
Intelligence for Building

Zabezpieczenia w systemie kontroli dostępu RACS 5

System kontroli dostępu RACS 5 oferuje wielowarstwowy system zabezpieczeń, którego celem jest jego przeciwdziałanie próbom ominięcia zasad kontroli ruchu osób i wyposażenia dla realizacji, których został on w dozorowanym obiekcie zainstalowany. Na system zabezpieczeń składają się trzy główne elementy: wykorzystanie identyfikatorów zabezpieczonych przed duplikowaniem, szyfrowanie wszystkich rodzajów komunikacji stosowanych w systemie, kontrolowany dostęp do jego oprogramowania zarządzającego.

W ofercie systemu RACS 5 dostępna jest duża grupa czytników serii MCTxxM obsługujących karty zbliżeniowe MIFARE®, w tym karty typu DESFire oraz Plus oferujące najwyższy stopień zabezpieczeń szyfrujących. Kod karty MIFARE® może być przechowywany w szyfrowanych sektorach jej pamięci, przez co nie jest możliwe jego odczytanie, a tym samym zduplikowanie nawet w przypadku fizycznego dostępu do karty. Zarówno hasło szyfrujące kod karty jak i lokalizacja miejsca jego przechowywania na karcie MIFARE® podlegają indywidualnemu programowaniu, co powoduje, że karty z obcych systemów nie działają w danej instalacji kontroli dostępu. Opcjonalnie, karty MIFARE® można tak skonfigurować, że będzie możliwe ich wykorzystanie w wielu aplikacjach (systemach) niemniej tak długo jak kod karty będzie przechowywany w osobnym sektorze danych i zabezpieczony tajnym hasłem poziom bezpieczeństwa systemu kontroli dostępu nie będzie obniżony.

W systemie RACS 5 dostępna jest tzw. mobilna identyfikacja użytkowników, która umożliwia wykorzystanie telefonu, jako identyfikatora. Również w tym przypadku, komunikacja pomiędzy telefonem wykorzystywanym dla celów identyfikacji użytkownika a czytnikiem podlega szyfrowaniu, a jej podsłuchanie nie stwarza zagrożenia dla bezpieczeństwa.

Kolejnym zabezpieczeniem, są tzw. wieloetapowe tryby identyfikacji użytkowników, które wymuszają użycie więcej niż jednej formy identyfikacji. System oferuje zarówno typowe wbudowane tryby identyfikacji takie jak „Karta + PIN" oraz „Karta + Odcisk palca", a dodatkowo umożliwia tworzenie własnych bardziej złożonych trybów np. „Karta + PIN + Linie papilarne". W ofercie systemu RACS 5 znajduje się czytnik linii papilarnych RFT1000, który umożliwia przechowywanie wzorców odcisków papilarnych w swojej wewnętrznej pamięci lub na karcie zbliżeniowej MIFARE®, którą posługuje się użytkownik.

Zastosowanie kart zbliżeniowych MIFARE® w połączeniu z wielostopniowymi trybami identyfikacji tworzy bardzo wysoką barierę bezpieczeństwa, która może być dodatkowo wzmocniona funkcją „Dostępu z autoryzacją zewnętrzną" oraz funkcją „Wejścia komisyjnego". Pierwsza z wymienionych funkcji uzależnia ostateczną decyzję o przyznaniu dostępu od operatora śledzącego pracę systemu, który może wizualnie np. przy użyciu obrazu z kamer zidentyfikować osobę i zaakceptować przyznanie dostępu. W przypadku drugiej z wymienionych funkcji dostęp może być przyznany dopiero po identyfikacji dwóch użytkowników uprawnionych do danego przejścia.

Komunikacja pomiędzy oprogramowaniem zarządzającym systemem a kontrolerami dostępu jest realizowana przez sieć komputerową i jest szyfrowana metodą AES128 CBC. Metoda ta polega na szyfrowaniu komunikacji przy pomocy dynamicznie zmieniającego się hasła, co z jednej strony czyni przesyłane ramki nieczytelne, a z drugiej blokuje możliwość sterowania systemem przez ich replikację. Komunikacja wewnętrzna pomiędzy kontrolerem dostępu a czytnikami i innymi modułami może być realizowana przewodowo przez magistralę RS485, sieć komputerową, a także bezprzewodowo (drogą radiową). W każdym z tych przypadków jest ona szyfrowana i podobnie jak komunikacja po sieci LAN jest zabezpieczona przed jej replikowaniem.

Dostęp do oprogramowania obsługującego system wymaga uwierzytelnienia hasłem. System może być obsługiwany przez wielu operatorów z różnymi poziomami uprawnień. Działania operatorów są rejestrowane w dedykowanym do tego celu dzienniku zdarzeń, który może stanowić cenne źródło danych w przypadku potrzeby odtworzenia biegu wypadków związanych z zarządzaniem, konfiguracją i obsługą systemu.

Uwaga!
W odróżnieniu od powszechnie spotykanych w handlu czytników kart standardu MIFARE®, czytniki serii PRTxxMF oraz MCTxxM (ROGER) posiadają możliwość pracy zarówno z nieszyfrowanym kodem karty (tzw. kod CSN) jak i kodem szyfrowanym (tzw. kod SSN). W przypadku, gdy system kontroli dostępu wykorzystuje kod CSN karty MIFARE® lub karty EM 125 kHz, jest on zagrożony możliwością klonowania kart, co stanowi bardzo krytyczne obniżenie jego poziomu bezpieczeństwa. W systemach, w których klonowanie kart jest zbyt istotnym zagrożeniem należy stosować czytniki z szyfrowanym kodem karty (np. czytniki serii MCTxxM ROGER) skonfigurowane do pracy z kodem SSN.

Charakterystyka:
- Szyfrowana komunikacja sieciowa
- Szyfrowana komunikacja na magistrali RS485
- Szyfrowana komunikacja radiowa
- Szyfrowana baza danych
- Szyfrowana komunikacja NFC
- Szyfrowana komunikacja Bluetooth
- Szyfrowane oprogramowanie kontrolerów dostępu
- Szyfrowane kody kart (MIFARE® SSN)
- Identyfikacja biometryczna za pośrednictwem linii papilarnych
- Wieloetapowe tryby identyfikacji użytkownika
- Zewnętrzna autoryzacja dostępu
- Tryb wejścia komisyjnego
- Logowanie do oprogramowania zabezpieczone loginem i hasłem
- Konfigurowalne poziomy uprawnień operatorów systemu
- Rejestracja działań operatorów systemu

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

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