RACS 5

Access Control
and Building
Automation System

Sikkerhed i adgangskontrol system

Krypteret database

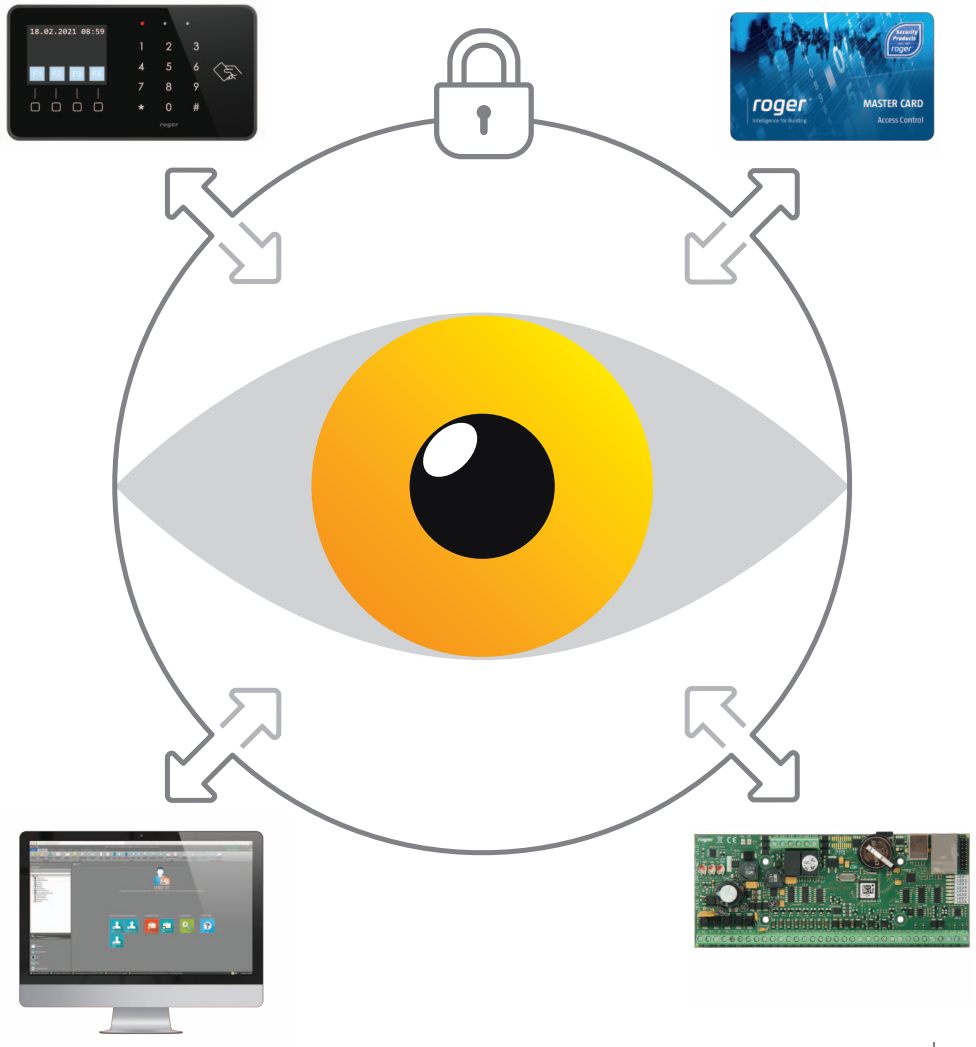
Krypteret kommunikation mellem software og enheder

Adgangsniveauer i RACS 5 administrations software og operatør identifikation

Krypterede proxkort numre

Biometrisk identifikation af brugere

Flertrins identifikation af brugere



roger
Intelligence for Building

RACS 5 | Access Control and Building Automation System

Sikkerhed i adgangskontrol system

RACS 5 systemet muliggør sikkerhed i flere lag for at forhindre overtrædelse af adgangsrettigheder af brugere og aktiver i det område, som systemet dækker. Sikkerheden i systemet består af tre hovedelementer: brugen af identifikations faktorer sikret mod kopiering, kryptering af alle typer af kommunikation, der anvendes i systemet, kontrolleret adgang til administrations software.

RACS 5 systemet tilbyder et stort udvalg af MCTxxM serie læsere, der understøtter MIFARE® proxkort, herunder DESFire og Plus kort med det højeste niveau af krypteringssikkerhed. MIFARE® korts kode kan lagres i de krypterede sektorer i hukommelsen, så det er ikke muligt at læse den og dermed duplikere det, selv med fysisk adgang til kortet. Både adgangskoden krypteringen af kortkoden og dens placering i MIFARE® Card hukommelse programmeres individuelt, hvilket betyder, at kortene fra andre systemer ikke kan fungerer i adgangskontrol installationen. MIFARE® kort kan eventuelt konfigureres, så de kan benyttes i mange installationer (systemer) men så længe kort koderne lagres i en separat data sektor og sikres med adgangskoder, reduceres sikkerhedsniveauet for adgangskontrolsystemet ikke.

RACS 5 giver mulighed for at identificere brugere med deres mobile enheder. I sådanne tilfælde er kommunikationen mellem mobilenheden og RACS 5 terminalen krypteret, og scanning af transmissionen udgør ikke en trussel mod sikkerheden.

En anden tilgængelig sikkerhedsforanstaltning består i flertrins brugergodkendelses tilstande, der kræver brug af mere end én form for identifikation. Systemet tilbyder både typiske indbyggede identifikations tilstande som "kard + PIN" og "kard + fingeraftryk", og muliggør også konfiguration af dine egne komplekse tilstande, f.eks. "kard + PIN + fingeraftryk". RACS 5 systemet indeholder RFT1000 fingeraftrykslæser, som kan gemme fingeraftryks skabeloner i hukommelsen eller kan benytte skabeloner, der er gemt i hukommelsen i MIFARE® kort.

Brugen af MIFARE® proxkort i kombination med flertrins brugergodkendelses tilstande skaber en meget høj sikkerhedsbarriere, som yderligere kan styrkes af funktionen "adgang ved fjern autorisation" og funktionen "to-bruger indtastning". Den første gør adgang tildeling afhængig af operatør accept, der kan bruge CCTV kameraer til visuelt at identificere en bruger, før fjernadgang tildeles. I tilfælde af den anden funktion kan der kun gives adgang efter identifikation af to godkendte brugere.

Kommunikationen mellem systemets administrations software (VISO) og adgangs kontrollere udføres via et computer netværk (LAN) og krypteres ved hjælp af AES128 CBC metoden. Denne metode består i kryptering af kommunikation ved hjælp af en dynamisk skiftende adgangskode, som gør det transmitterede uforståeligt og samtidig forhindrer kopiering af dem. Intern kommunikation mellem adgangs kontrolleren og læserne og/eller andre moduler kan foregå med RS485 bus, computernetværk og trådløst. I hver af disse tilfælde er det krypteret og på samme måde som LAN kommunikation med kontrolleren er det beskyttet mod kopiering. Adgang til administrator software (VISO) kræver godkendelse med adgangskode. Systemet kan betjenes af mange administratorer med forskellige autorisationsniveauer. Operatør handlinger registreres i en dedikeret hændelseslog. Dette kan være meget nyttigt, når det er nødvendigt at rekonstruere forløbet af begivenheder i forbindelse med forvaltning, konfiguration og drift af systemet.

Bemærk!
I modsætning til standard MIFARE® kortlæsere, der almindeligvis udbydes på markedet, kan PRTxxMF og MCTxxM (Roger) seriens læsere benyttes både med ikke-krypterede (CSN) og krypterede (SSN) kortnumre. Hvis bruger id i adgangskontrolsystemet er baseret på EM 125 kHz eller MIFARE® (CSN) kort, er der risiko for kort kloning, hvilket udgør et meget kritisk fald i sikkerhedsniveauet. I systemer, hvor kort kloning er en væsentlig trussel, bør læserne med en krypteret kort kode (SSN) benyttes (f.eks. læsere fra MCTxxM Roger serien).

Funktioner:
- Krypteret computer netværkskommunikation
- Krypteret RS485 bus kommunikation
- Krypteret trådløs kommunikation
- Krypteret database
- Krypteret NFC kommunikation
- Krypteret Bluetooth kommunikation
- Krypteret firmware til adgangs kontrollere
- Understøttelse af krypterede kortnumre (MIFARE® SSN)
- Biometrisk identifikation med fingeraftryk
- Flertrins godkendelsestilstande for brugere
- Adgang ved fjerngodkendelse
- To-brugere indtastnings metode
- System administrations software beskyttet med login og kodeord
- Konfigurérbare adgangsniveauer for operatører af system administrations software
- Operatør handlinger, registreres i dedikeret logfil

Distribution:

Pro Sec A/S
Professional Security

Pro-Sec A/S
Egegårdsvej 11
4621 Gadstrup
Denmark

T. +45 56 130 630
E. info@pro-sec.dk
www.pro-sec.dk

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

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

roger