System Zdalnego Ryglowania

System Zdalnego Ryglowania eliminuje praktycznie w 99% konieczność dostarczania kluczy w tradycyjnym sposobie otwierania i zamykania placówek bankowych. System został zbudowany konkretnie do tego celu z uwzględnieniem wszelkich standardów komunikacyjnych i bezpieczeństwa. Sercem systemu jest specjalizowany kontroler odpowiedzialny za komunikację z klawiaturą kodową wyposażoną w czytnik kart, elektro-zamkiem i połączeniem LAN/WAN z Alarmowym Centrum Odbiorczym, jak również z zapasowym nadajnikiem wspierającym transmisję GPRS/SMS. Kontroler realizuje także zadania związane z przyjmowaniem i aktualizowaniem użytkowników uprawnionych do zdalnego ryglowania oraz rozkazami awaryjnego otwarcia.

Zastosowanie:

- otwierania i zamykania placówek bankowych,
- otwierania i zamykania dużych serwerowni,
- kontrolowania dostępu do przed-skarbców,
- kontrolowania dostępu do stref szczególnie chronionych.

CMA MONITORING
EKSPERCI OD MONITORINGU
www.cma.com.pl

ul. Puławska 359, 02-801 Warszawa
+48 (22) 546 08 88
info@cma.com.pl

NIP 951 10 01 175
KRS 0000 384727
REG 011311220

Funkcjonalności

- Umożliwienie przeprowadzenia zdalnej kontroli uprawnień w procesie otwierania lub zamykania placówek bankowych z uwzględnieniem występowania dwu-osobowych komisji złożonych z upoważnionych do tego celu pracowników Banku.
- Zapewnienie bez kluczowego otwarcia lub zamknięcia drzwi wejściowych do placówek Banku.
- Możliwość wykonania procedury tzw. awaryjnego otwarcia lub zamknięcia wynikającego z konieczności działania w procesie ryglowania po za godzinami pracy i w sytuacjach wyjątkowych.
- Udostępnienie zewnętrznego interfejsu dla kadry kierowniczej placówek bankowych, połączonego bezpośrednio z systemem Alarmowego Centrum Odbiorczego w celu umożliwienia wprowadzania lub usuwania uprawnień osób upoważnionych do zdalnego ryglowania.
- Zapewnienie bezpieczeństwa w zakresie szyfrowania komunikacji w dowolnym torze transmisji, zapewnienia ochrony przed podmianą urządzeń transmisyjnych, raportowania zdarzeń związanych z obsługą systemu oraz ochroną antysabotażową.
- Tworzenia raportów dla Biura Bezpieczeństwa Banku związanych z działaniem systemu i kontrolą zmian danych osób upoważnionych.
- Ochrona kodów osobistych przed ujawnieniem polegająca na ochronie przed odczytaniem ich przez innych użytkowników systemu, administratorów, operatorów ACO, instalatorów.
- Uniezależnienie systemu od obecnych w sieci bankowej urządzeń z dziedziny zabezpieczeń elektronicznych.
- Zastosowanie specjalnego elektrozamka dowolnego producenta z uwzględnieniem funkcji ryglowania mechanicznego.