

Wymagania funkcjonalne systemu kontroli dostępu (KD)

1. Ogólne wymagania dotyczące systemu KD

- a. System KD musi być systemem otwartym, co oznacza działanie na kontrolerach ogólnie dostępnych dla producentów KD, umożliwiając wymianę oprogramowania KD i wykorzystanie kontrolerów przez innych producentów.
- b. System musi być łatwo rozbudowywany po zakończeniu gwarancji przez dowolną firmę korzystającą z tych samych kontrolerów.
- c. Obsługa kontrolerów co najmniej czterech różnych producentów oraz zamków bezprzewodowych co najmniej dwóch producentów.
- d. Integracja z co najmniej czterema systemami zarządzania wideo (VMS), dostępnymi i wspieranymi lokalnie.

2. Wymagania dotyczące czytników i identyfikacji użytkowników

- a. Obsługa czytników niezależnych producentów działających w standardzie OSDP.
- b. Szyfrowanie połączenia z kontrolerem bez dodatkowych urządzeń korzystających z nieszyfrowanych protokołów (np. Wiegand).
- c. Obsługa kart działających na częstotliwości 13,56MHz; częstotliwość 125kHz nie może być aktywna w systemie KD.
- d. Szablony ustawień dla diody LED i brzęczyka dla czytników kart (OSDP).
- e. Obsługa mobilnych czytników do kontroli użytkowników w trybie online i offline (np. kontrola na korytarzu lub podczas ewakuacji).
- f. Możliwość przygotowania raportu o liczbie osób w obiekcie podczas alarmu pożarowego.
- g. Asysta gości – użytkownik z kartą gościa musi przemieszczać się pod nadzorem osoby uprawnionej.

3. Architektura systemu i integracje

- a. Wykorzystanie istniejącej infrastruktury sieciowej bez potrzeby dodatkowych linii komunikacyjnych.
- b. Możliwość zastosowania modułów rozszerzeń.
- c. Integracja z centralami alarmowymi SWiN.
- d. Integracja z systemami nadzoru wizyjnego (VMS) na poziomie oprogramowania.
- e. Możliwość przechwycenia i wyświetlenia obrazu z kamery VMS umieszczonej przy drzwiach w momencie uzyskania dostępu.
- f. Wyświetlanie alarmów bezpieczeństwa i KD na mapie obiektu oraz sterowanie dostępem z poziomu mapy.
- g. Możliwość uzbrajania i rozbrajania strefy SWiN z poziomu czytnika kart RFiD.
- h. Obsługa sterowania windą i ograniczania dostępu do pięter według poziomów dostępu.

4. Wymagania dotyczące oprogramowania KD

- a. Interfejs użytkownika i funkcje administracyjne
 - o Graficzny interfejs użytkownika dostępny w języku polskim.
 - o Możliwość dostępu do wszystkich funkcji systemu przez przeglądarkę bez konieczności instalacji dodatkowego oprogramowania.

- Obsługa zarządzania systemem zdalnie przez Internet oraz poprzez dedykowaną aplikację mobilną (Android/iOS).
 - Możliwość zarządzania użytkownikami i sterowania drzwiami poprzez aplikację mobilną.
 - Obsługa minimum 5 zestawów identyfikatorów dla jednego użytkownika (np. karta RFID, kod PIN, kod QR, aplikacja mobilna, numer rejestracyjny pojazdu).
- b. Monitorowanie i raportowanie
- Moduł monitorujący wizualizację zdarzeń dostępowych wraz ze zdjęciami użytkowników.
 - Moduł alertów z możliwością harmonogramowania, komentowania i rejestrowania działań operatora.
 - Rejestracja Czasu Pracy (RCP) oraz raporty zdarzeń, dostępu do drzwi, czasu i frekwencji, listy użytkowników.
 - Rejestracja wszystkich czynności wykonywanych przez operatora z możliwością audytu.
 - Indywidualne przyznawanie dostępu do stref i drzwi na podstawie ról użytkowników.
- c. Integracje i automatyzacja
- Mechanizm automatyzacji akcji oparty na regułach "If This, Then That" (IFTTT).
 - Wysyłanie i odbieranie powiadomień poprzez REST API do innych systemów.
 - Obsługa powiadomień e-mail i automatycznych scenariuszy kontroli dostępu.
 - Interfejs wymiany danych z zewnętrznymi systemami zarządzania przedsiębiorstwem i RCP.
 - Moduł importu użytkowników (Microsoft Active Directory, CSV).
 - Możliwość synchronizacji użytkowników z systemami zarządzania przedsiębiorstwem.
 - Integracja z systemem rezerwacji sal.

5. Bezpieczeństwo i zarządzanie danymi

- a. Logiczna segmentacja bazy danych umożliwiająca przypisanie użytkowników, drzwi i kamer do określonych segmentów.
- b. Konfigurowalny pulpit graficzny do monitorowania zdarzeń w czasie rzeczywistym.
- c. Obsługa bezpłatnej, komercyjnej bazy danych SQL (np. PostgreSQL).
- d. Automatyczna konserwacja, czyszczenie i tworzenie kopii zapasowych bazy danych.
- e. Kalendarz praw dostępu pozwalający na czasowe ograniczenia (np. urlopy, święta).

6. Sprzętowe funkcje systemu KD

- a. Obsługa anti-passback, trybu klasowego (Classroom Mode), sterowania dwiema kartami dla czytnika wejściowego.
- b. Obsługa limitu wejść oraz odblokowania pierwszej karty do aktywacji harmonogramu wejść.
- c. Obsługa komend z klawiatury czytnika (funkcja "locker" – sterowanie wieloma wyjściami z jednego czytnika).
- d. Możliwość sterowania szlabanem parkingowym na podstawie numerów rejestracyjnych pojazdów. LPR (License Plate Recognition) nie powinien wymagać zastosowania systemu VMS
- e. Obsługa minimum 5 numerów rejestracyjnych przypisanych do użytkownika.

7. API i otwartość systemu

- a. Bezpłatne API umożliwiające integrację z innymi systemami.
- b. Preferowane jest ustandaryzowane REST API.
- c. Obsługa kluczy kryptograficznych, których właścicielem i dysponentem jest zamawiający.
- d. Możliwość dodawania czytników i kart bez ograniczeń ze strony instalatora lub producenta KD.

Wymagania funkcjonalne dotyczące oprogramowania systemu telewizji dozorowanej

1. Architektura systemu

- a. System VMS musi być otwartą platformą umożliwiającą integrację z urządzeniami wielu producentów.
- b. VMS musi wspierać integrację z różnymi systemami kontroli dostępu oraz systemu sygnalizacji włamania i napadu (SSWiN).
- c. System musi zapewnić możliwość współpracy z oprogramowaniem do zarządzania kontrolą dostępu, umożliwiając synchronizację użytkowników, uprawnień oraz rejestrowanie zdarzeń dostępowych.
- d. VMS musi działać w architekturze klient-serwer.
- e. System musi wspierać instalację w środowiskach wirtualnych.

2. Skalowalność i elastyczność

- a. VMS musi umożliwić nieograniczoną rozbudowę systemu, bez limitu serwerów i połączeń urządzeń.
- b. W początkowej wersji system musi obsługiwać co najmniej 64 urządzenia.
- c. System nie może ograniczać liczby jednoczesnych połączeń użytkowników.

3. Aplikacje klienckie i dostęp

- a. VMS musi oferować aplikacje klienckie dla:
 - Systemu Windows,
 - Urządzeń mobilnych z systemami iOS i Android,
 - Dostęp poprzez interfejs webowy.
- b. Oprogramowanie klienckie musi być dostępne bez dodatkowych opłat dla użytkowników.

4. Funkcjonalności zarządzania i monitoringu

- a. System musi umożliwiać zarządzanie użytkownikami, w tym nadawanie uprawnień dostępu do kamer i nagrań.
- b. VMS musi obsługiwać strumieniowanie na żywo oraz nagrywanie materiału wideo.
- c. Wymagana jest możliwość przeglądania archiwalnych nagrań z opcją ich eksportu.
- d. System musi obsługiwać powiadomienia alarmowe w przypadku wykrycia zdarzeń (np. ruch, wtargnięcie, manipulacja przy kamerze).
- e. VMS powinien umożliwiać zdalne sterowanie kamerami PTZ.

5. Obsługa metadanych i analityki wideo

- a. System musi obsługiwać metadane generowane przez kamery wyposażone w analitykę wideo.
- b. System powinien umożliwiać przeszukiwanie nagrań w oparciu o metadane (np. detekcja ruchu, rozpoznawanie twarzy, tablic rejestracyjnych).

6. Integracja z systemami kontroli dostępu i alarmowymi

- a. System musi zapewnić możliwość integracji z oprogramowaniem do zarządzania kontrolą dostępu, umożliwiając synchronizację użytkowników, uprawnień oraz rejestrowanie zdarzeń dostępowych.
- b. VMS musi obsługiwać protokoły umożliwiające integrację z systemami kontroli dostępu i alarmowymi.
- c. System musi umożliwiać wymianę danych z innymi systemami poprzez API, w tym synchronizację zdarzeń rejestrowanych przez VMS z rejestrem zdarzeń dostępowych.

Wymagania funkcjonalne dotyczące urządzeń

1. Klamki bezprzewodowe

a. Wymagane technologie RFiD:

- Klamki bezprzewodowe muszą obsługiwać następujące technologie identyfikacji radiowej (RFiD):
- iCLASS
- iCLASS SE
- iCLASS Seos
- MIFARE Classic
- MIFARE Classic SE
- MIFARE Ultralight
- MIFARE Plus
- MIFARE DESFire 0.6
- MIFARE DESFire EV1
- MIFARE DESFire EV2 (w trybie Legacy mode)
- MIFARE DESFire EV3 (w trybie Legacy mode)
- MIFARE DESFire SE
- PicoPass
- ISO 14443A UID
- ISO 14443B UID
- ISO 15693 UID

b. Wymagane technologie mobilne:

Klamki bezprzewodowe muszą obsługiwać technologię HID Mobile Access, umożliwiającą autoryzację dostępu przy użyciu urządzeń mobilnych.

c. Tryb pracy:

Urządzenia muszą działać w trybie online, umożliwiając zdalne zarządzanie i monitorowanie dostępu w czasie rzeczywistym.

d. Bezpieczeństwo komunikacji:

- Komunikacja bezprzewodowa między klamkami a systemem zarządzania dostępem musi być szyfrowana przy użyciu 128-bitowego szyfrowania.
- Standard radiowy wykorzystywany do komunikacji musi spełniać normę IEEE 802.15.4 (2.4 GHz), zapewniając stabilność oraz odporność na zakłócenia.

2. Kontrolery

a. Wymagania komunikacyjne:

- Obsługa protokołów komunikacyjnych IPv4/6, TLS 1.2 oraz 802.1X.
- Komunikacja z czytnikami kontroli dostępu poprzez OSDP.
- Komunikacja z HUB-ami klamek bezprzewodowych za pośrednictwem TCP/IP, z szyfrowaniem TLS 1.1/1.2.

b. Wymagania dodatkowe:

- Kontrolery należy dostarczyć z zasilaczami buforowymi.
- Kontrolery muszą być dostarczone w odpowiednich obudowach, zapewniających ochronę urządzeń i łatwość instalacji.

3. Czytnik kontroli dostępu

- a. Komunikacja z kontrolerem musi odbywać się za pośrednictwem protokołu OSDP.

b. Wymagane technologie RFiD:

- Seos®
- iCLASS SE®
- iCLASS SR®
- iCLASS®
- MIFARE Classic
- MIFARE DESFire EV1/EV2/EV3
- FeliCa™ & Contactless e-Purse Application Specification (CEPAS)
- Mobile Credentials powered by Seos (HID Mobile Access)

c. Wymagania dodatkowe:

- Czytnik musi posiadać klawiaturę umożliwiającą wprowadzanie kodów dostępu.
- Musi obsługiwać technologię mobilną HID Mobile Access do autoryzacji dostępu za pomocą urządzeń mobilnych.

4. Węzły komunikacyjne (Hub)

- a. Urządzenie musi umożliwiać komunikację pomiędzy zamkami bezprzewodowymi, a pozostałymi elementami systemu kontroli dostępu
- b. Musi wspierać szyfrowaną komunikację radiową z zamkami z wykorzystaniem standard AES 128-bit
- c. Hub musi być kompatybilny z systemem zarządzania i zapewnić pełną integrację z kontrolerami
- d. Komunikacja z kontrolerami systemu musi odbywać się przy użyciu protokołu TCP/IP
- e. Hub musi posiadać certyfikaty CE oraz, jeśli wymagane – inne dokumenty zgodności wymagane dla urządzeń radiowych w UE

5. Kamera kopułowa wewnętrzna

- a. Przetwornik CMOS minimum 1/2.8 “
- b. Praca w kolorze przy minimalnym oświetleniu 0,1 lux
- c. Rozdzielczość 1920x1080
- d. Pole widzenia 100-36°
- e. Maksymalna ilość klatek na sekundę 50
- f. Video analiza rozpoznawanie obiektów. Alarm przebywanie w strefie
- g. Integracja z kontrolą dostępu.

6. Kamera kopułowa do rozpoznawania tablic

- a. Przetwornik CMOS minimum 1/2.8 “
- b. Praca w kolorze przy minimalnym oświetleniu 0,1 lux
- c. Rozdzielczość 1920x1080
- d. Pole widzenia 100-36°
- e. Maksymalna ilość klatek na sekundę 50
- f. Video analiza rozpoznawanie tablic rejestracyjnych, klasyfikacja pojazdów.
- g. Integracja z kontrolą dostępu.

7. Depozytor kluczy

- a. Musi umożliwić zabezpieczone przechowywanie min. 5 zestawów kluczy do samochodów;
- b. Każdy klucz ma być przypisany do indywidualnego gniazda lub skrytki z rejestracją operacji;

- c. Możliwość automatycznej identyfikacji, który klucz został pobrany/zwrócony;
- d. Urządzenie musi wspierać mechanizmy uwierzytelniania stosowane w systemie KD budynku;
- e. Musi umożliwiać pełną integrację z zewnętrznym systemem zarządzania zastosowanym w budynku;