

Inwestycja: **MODERNIZACJA BUDYNKU KOAGULACJI ZACHODNIEJ
I OSADNIKÓW POKOAGULACYJNYCH NA STACJI UZDATNIANIA
WODY PRZY UL. GÓRNEJ 56B W PŁOCKU
ul. Górna 56B, 09-402 Płock**

Zamawiający: **Wodociągi Płockie Sp. z o.o.
ul. Harcerza A. Gradowskiego 11, 09-402 Płock**

Autor dokumentacji: **AQUA S.A. ul. Kanclerska 28, 60-327 Poznań**

WWiOR-12

Instalacje teletechniczne

październik 2025 r.

ZAWARTOŚĆ OPRACOWANIA

1. DANE OGÓLNE.....	4
1.1. Inwestycja.....	4
1.2. Inwestor	4
1.3. Przedmiot i zakres robót budowlanych	4
1.4. Nazwy i kody CPV	4
1.5. Roboty tymczasowe i towarzyszące.....	4
1.6. Informacja o terenie budowy	4
1.7. Określenia podstawowe	4
2. WYMAGANIA DOTYCZĄCE WŁAŚCIWOŚCI WYROBÓW BUDOWLANYCH	5
2.1. Wymagania podstawowe	5
2.2. Funkcje systemu kontroli dostępu	5
2.2.1. Funkcja blokady / służowość	5
2.2.2. Funkcja blokady służowość „podstawowa”	5
2.2.3. Funkcja blokady / służowość „rozszerzona”	5
2.2.4. Funkcje bezpieczeństwa: osoba znajduje się zbyt długo w strefie	6
2.2.5. Zarządzanie zagrożeniami (poziom dostępu)	6
2.2.6. Karta dostępu: automatyczna dezaktywacja nieużywanej karty.....	7
2.2.7. Karta dostępu: karta strażaka „złota karta”	7
2.2.8. Antypassback (APB) - dozwolone tylko jedno żądanie dostępu	7
2.2.9. Scalanie / łączenie osób (merge persons)	7
2.3. Funkcje stacji operatorskiej i serwera	8
2.3.1. GRADE 3	8
2.3.2. Przechowywanie danych dostępu do zdarzeń	8
2.3.3. RODO - ochrona danych osobowych	8
2.3.4. Neutralność maszyny serwerowej	8
2.3.5. Wirtualizacja	8
2.3.6. ACTIVE DIRECTORY AD.....	9
2.3.7. Funkcja redundancji.....	9
2.3.8. Dwustopniowe uwierzytelnianie / autoryzacja operatora.....	9
2.3.9. Procedury i akcje	9
2.3.10. Procedury - obsługa wyrażeń regularnych w procedurze	10
2.3.11. Ilość zdarzeń w bazie SKD	10
2.3.12. Autoryzacja grupy użytkowników na podstawie lokalizacji stacji roboczej	10
2.3.13. Wirtualizacja, ikony widżety i filtry	10
2.3.14. Statystyka działania bazy danych.....	11
2.3.15. Powiadomienie o wygaśnięciu hasła dla konta operatora	11
2.3.16. Automatyczna dystrybucja firmware (Provisioning).....	11
2.3.17. Moduł wysłania transakcji za pomocą wiadomości „push”	11
2.4. Wymagane protokoły komunikacji.....	12
2.4.1. Wsparcie dla protokołu OSDP V2.2	12
2.4.2. Interpretacja kodowania kart	12
2.5. Wymagania sprzętowe	12
2.5.1. Serwer systemu	12
2.5.2. Czytnik kart zbliżeniowych	12
2.5.3. Sterownik sieciowy	13
2.5.4. Kontroler drzwi.....	13
2.5.5. Obudowa instalacyjna.....	13
2.5.6. Zasilacz.....	13
3. WYMAGANIA DOTYCZĄCE SPRZĘTU I MASZYN	14
4. WYMAGANIA DOTYCZĄCE ŚRODKÓW TRANSPORTU	14
5. WYMAGANIA DOTYCZĄCE WYKONANIA ROBÓT BUDOWLANYCH	14
5.1. Składowanie	14
5.2. Przygotowanie do prac montażowych.....	14
5.3. Montaż urządzeń.....	14
5.4. Prowadzenie przewodów	14
6. KONTROLA JAKOŚCI.....	15
6.1. Kontrola zastosowanych materiałów	15
6.2. Kontrola wykonanych robót	15
7. PRZEDMIAR I OBMIAR ROBÓT	15

8. ODBIÓR ROBÓT	15
9. ROZLICZENIE ROBÓT TYMCZASOWYCH I TOWARZYSZĄCYCH	15
10. DOKUMENTY ODNIESIENIA.....	15

1. DANE OGÓLNE

1.1. INWESTYCJA

Modernizacja budynku koagulacji zachodniej i osadników pokoagulacyjnych na stacji uzdatniania wody przy ul. Górnej 56b w Płocku

1.2. INWESTOR

Wodociągi Płockie Sp. z o.o. ul. Harcerza A. Gradowskiego 11, 09-402 Płock

1.3. PRZEDMIOT I ZAKRES ROBÓT BUDOWLANYCH

Przedmiotem niniejszych WWiOR są wymagania dotyczące wykonania i odbioru robót budowlanych związanych z wykonaniem instalacji teletechnicznych w ramach zadania:

"Modernizacja budynku koagulacji zachodnie i osadników pokoagulacyjnych na stacji uzdatniania wody przy ul. Górnej 56b w Płocku".

1.4. NAZWY I KODY CPV

Przedmiot zamówienia objęty niniejszym opracowaniem odpowiada następującym robotom budowlanym opisanym kodem Wspólnego Słownika Zamówień (CPV) wg Rozporządzenia Komisji Wspólnoty Europejskiej nr 213/2008:

- 45300000-0 Roboty instalacyjne w budynkach

1.5. ROBOTY TYMCZASOWE I TOWARZYSZĄCE

Informację o robotach tymczasowych i towarzyszących zawarto w **WWiOR-00** "Wymagania ogólne".

1.6. INFORMACJA O TERENIE BUDOWY

Informację o terenie budowy zawarto w **WWiOR-00** "Wymagania ogólne".

1.7. OKREŚLENIA PODSTAWOWE

Określenia podstawowe zgodnie z **WWiOR-00** "Wymagania ogólne".

2. WYMAGANIA DOTYCZĄCE WŁAŚCIWOŚCI WYROBÓW BUDOWLANYCH

2.1. WYMAGANIA PODSTAWOWE

Ogólne wymagania dotyczące materiałów podano w specyfikacji **WWiOR-00** "Wymagania ogólne".

Dostawa urządzeń składających się na kompletny system kontroli dostępu musi obejmować poza urządzeniami również:

- montaż (urządzeń, zasilania, okablowania, oprogramowania, licencji, itp.);
- zaprogramowanie i testowanie działania systemu;
- uruchomienie;
- dokumentację powykonawczą;
- instrukcje eksploatacji i szkolenie służb Użytkownika.

2.2. FUNKCJE SYSTEMU KONTROLI DOSTĘPU

2.2.1. Funkcja blokady / służowość

System KD musi umożliwiać zaimplantowanie funkcji służowości podstawowej i rozszerzonej.

Służowość podstawowa „1 warunek” - Minimalnym elementem monitorującym spełnienie warunków służowości to stan otwartości drzwi weryfikowany za pomocą sygnału z kontaktronu.

Służowość rozszerzona „1, 2 lub 3 warunki” - System musi umożliwiać skonfigurowanie funkcjonalności służowości rozszerzonej, gdzie monitoring otwartości drzwi oprócz sygnału z kontaktronu uzupełniony jest o sygnał stanu rygla oraz stanu wykładki (zamka/cylindra). Każdy z w/w sygnałów musi posiadać w systemie osobny typ zdarzenia z możliwością raportowania. Niedopuszczane są rozwiązania zrównoleglenia w/w sygnałów na poziomie fizycznym/sztynno-drutowym.

2.2.2. Funkcja blokady służowość „podstawowa”

System KD musi umożliwiać zaimplantowanie funkcji służowości w podstawowej konfiguracji tzn.:

- możliwość tworzenia blokady przejść (służowości) dla minimum 32 czytników.
- służowość musi być funkcjonalnością lokalną danego kontrolera IP, który zarządza sterownikami drzwiowymi.
- służowość musi działać niezależnie w przypadku braku połączenia z serwerem głównym.
- system musi umożliwiać konfigurowanie grup służowości z możliwością:
 - zdalnego otwarcia przejścia przez operatora mimo niespełnienia warunków służowości przez wszystkie drzwi,
 - blokowanie możliwości zdalnego otwarcia przejścia przez operatora mimo niespełnienia warunków służowości,
 - kontrolery KD muszą umożliwiać podłączenie wejścia awaryjnego/wejścia wysokiego priorytetu, który umożliwi odblokowanie drzwi mimo niespełnienia warunków służowości.

2.2.3. Funkcja blokady / służowość „rozszerzona”

Rozszerzona funkcja służowości musi działać dla 32 czytników/32 przejść i mieć możliwość sprawdzenia stanu:

- położenia drzwi/kontaktron (door position),
- zasuwy drzwi/rygla (deadbolt),
- wejścia wkładki cylindrycznej (cylinder input).

Musi być możliwość konfiguracji:

- dla wybranych drzwi na potrzebę służowości trzeba sprawdzać wszystkie trzy, dwa lub tylko jeden stan;
- warunku czy operator może zdalnie (z wizualizacji) otwierać drzwi pomimo niespełnienia warunków służowości np. inne drzwi z grupy otwarte lub czy operator musi przestrzegać zasad służowości;
- operator może mieć możliwość otwarcia wielu drzwi z jednej grupy służowości;
- konfiguracji awaryjnych wejść „emergency input” dla wszystkich przejść w służbie. Wejście awaryjne zmienia stan pracy czytnika w tryb otwarcia awaryjnego, które wysteruje wyjście otwarcia drzwi, mimo braku spełnienia warunków w służbie. Wejście awaryjne jest nadrzędne do warunków służowości.

2.2.4. Funkcje bezpieczeństwa: osoba znajduje się zbyt długo w strefie

System KD musi posiadać możliwość wykrywania, czy osoba nie znajduje się zbyt długo w danych obszarach bez wychodzenia. Jeżeli osoba znajduje się w jednym lub wielu obszarach zbyt długo, system musi umożliwić wygenerowanie zdarzeń, które mogą wywołać procedurę dla dalszych działań na tym wydarzeniu.

Funkcja może być wykorzystana np. do weryfikacji osób pracujących samodzielnie.

Wymagane scenariusze konfiguracyjne i funkcjonalne:

- ustawienie indywidualne dla każdej osoby o maksymalnym czasie przebywania we wszystkich obszarach,
- ustawienia indywidualne dla obszarów o maksymalnym czasie przebywania w danym obszarze,
- możliwość użycia obu ustawień równolegle,
- generowanie zdarzenia/eventu typu „Osoba XXX zbyt długo przebywająca w obszarze XXX” i powiadomienie operatora,
- ustawienie minimalnego czasu przybywania w obszarze dla wartości 60 s,
- ustawienie maksymalnego czasu przybywania w obszarze, co najmniej 48 godzin.

2.2.5. Zarządzanie zagrożeniami (poziom dostęp)

System KD musi posiadać funkcjonalność Zarządzania zagrożeniami (Threat management), która na podstawie aktualnego stopnia zagrożenia w obiekcie umożliwia minimum:

- dynamiczną zmianę poziomów dostępu (uprawnień),
- dynamiczny sposobu działania czytników SKD.

Funkcjonalność „zarządzania zagrożeniami”:

- musi udostępniać możliwość wprowadzenia wielu scenariuszy w logikę systemu KD np. poziom ALPHA, BRAVO, CHARLIE, DELTA,
- każdy scenariusz musi mieć możliwość sterowania sposobem działania czytników KD np.
- nie używać kodu PIN w trybie ALPHA, używać kody PIN w trybie BRAVO i wyższym,
- używać normalnego trybu pracy czytnika w trybie ALPHA,
- przełączyć czytnik w trybu pracy „z potwierdzeniem” tzn. autoryzacji przez operatora w trybie CHARLIE i wyższym,
- możliwość blokowania uprawnień dostępu określonych grup osób na przykład gości, pracowników zewnętrznych,
- maksymalny poziom dostępu musi być przypisany do każdej osoby indywidualnie,

Funkcjonalność „zarządzanie zagrożeniami” musi być oparta o strefy/obszary KD co oznacza, że:

- każdy czytnik musi mieć możliwość przypisania indywidualnego obszaru wejścia do obszaru X oraz wyjścia do obszaru Y,
- każdy obszar musi mieć możliwość przypisania innego poziomu zagrożenia np. Budynek A - cały budynek może mieć ustawiony poziom BRAVO; budynek B - parter budynku B ma

mieć ustawnym poziom BRAVO, piętro 1 budynku B ma mieć ustawiony poziom CHARLIE, serwerownia, która mieści się w budynku B na 1 piętrze na mieć ustawiony poziom DELTA,

- zmiana poziomu zagrożenie musi być wyzwalana min. za pomocą:
 - Wejścia stykowego na kontrolerze drzwiowym np. przycisk SOS,
 - Przycisku na wizualizacji systemu KD,
 - Sygnał z systemu „trzeciego” np. PSIM,
 - Przyłożenia karty dostępowej o specjalnym identyfikatorze.

2.2.6. Karta dostępowej: automatyczna dezaktywacja nieużywanej karty

System KD musi umożliwiać ustawienie czasu do automatycznej dezaktywacji karty z powodu nieużywania karty. W szczegółach karty użytkownika musi być wyświetlana ilość dni, która pozostała do automatycznej dezaktywacji kart.

2.2.7. Karta dostępowej: karta strażaka „złota karta”

System KD musi posiadać możliwość konfiguracji karty dostępowej z tzw. funkcją karty strażaka. Funkcja pomaga wprowadzać ustawienia priorytetowe dla dostępu dla strażaków lub innych osób, które mogą być zaangażowane w sytuacje awaryjne na obiekcie.

Aktywacja funkcji karty strażaka w systemie KD dla wybranej karty powoduje, że karta posiada najwyższy priorytet z automatycznymi ustawieniami dla kategorii takich jak:

- ważności karty: Tak (zawsze TAK),
- okres ważności karty: bez limitu,
- czasowy AntyPassBack: Wyłączony,
- automatyczna dezaktywacja karty, gdy używana dłużej niż: karta zawsze aktywna,
- brak ograniczeń dla obszarów o ograniczonym dostępie np.: ilości osób w strefie.

2.2.8. Antypassback (APB) - dozwolone tylko jedno żądanie dostępu

System KD musi posiadać weryfikację czy karta zbliżeniowa ma już oczekujące żądanie dostępu na innym czytniku podczas stosowanie funkcji APB.

W praktyce, gdy istnieje obok siebie wiele wejść opartych o tripod, funkcja ta sprawdza, czy dana karta jest używana tylko na jednym czytniku/tripodzie w tym samym czasie.

Jeśli ta funkcja nie jest aktywna, możliwe jest otwarcie dwóch przejść, jeśli z punktu widzenia systemu KD osoba nadal znajduje się na zewnątrz strefy APB, w innej strefie KD np.: wejście hol windy.

Oznacza to, że zmiana lokalizacji strefy APB w systemie KD jest wykonywana dopiero po zmianie stanu wejście położenia drzwi/kontaktronu/bramki tripod.

Funkcja musi działać lokalnie tzn. w obszarze jednego kontrolera IP dla minimum 32 przejść/czytników.

W przypadku użycia karty na co najmniej 2 czytaniach system KD musi wygenerować zdarzenie o treści np.: dostęp do czytnika: brak dostępu => karta jest już przetwarzana na innym czytniku.

2.2.9. Scalanie / łączenie osób (merge persons)

System KD musi posiadać możliwość łączenia/scalania wielu osób w jedną osobę w bazy danych KD. Dotyczy to przypadków, gdy, że użytkownik został wielokrotnie dodany do bazy danych. W praktyce Może się to zdarzyć przy błędach w pisowni nazwiska/imienia lub z różnymi poświadczeniami lub prawami dostępu. Łączenie osób w praktyce musi działać w następujący sposób:

- należy wybrać/zaznaczyć osoby „rekordy” do scalenia,
- aktywować funkcje scalania.

Pierwszy wybrany rekord będzie rekordem wiodącym, a wszystkie podstawowe dane (klucze dostępu, informacje kontaktowe itp.) zostaną dodane do konta użytkownika.

2.3. FUNKCJE STACJI OPERATORSKIEJ I SERWERA

2.3.1. GRADE 3

System SKD musi być zgodny z EN 60839 GRADE3. Stopień GRADE musi być potwierdzony przez producenta systemu KD za pomocą oświadczenia oraz za pomocą świadectwa kwalifikacyjnego wydanego przez TECHOM.

2.3.2. Przechowywanie danych dostępu do zdarzeń

System KD musi posiadać funkcje audytu tzn.: logowanie w systemie KD prób wyświetlania/drukowania logów systemu KD przez operatora danego operatora. Zgodnie z wymaganiem normy EN60839-11 Grade 3 i 4 system musi posiadać mechanizm audytu/logowania informacji, który operator szukał, wyświetlał dane historyczne systemu KD.

Dane, które mają się logować to minimum ID operatora oraz data i godzina wyszukiwania zdarzeń.

2.3.3. RODO - ochrona danych osobowych

Zgodnie z RODO dane osobowe muszą być chronione przed wszelkimi przypadkami nadużycia w najlepszym możliwy sposób. Dane osobowe mogą być zapisane w bazie danych SKD, z tego powodu baza danych i kopia zapasowa bazy danych musi być zabezpieczona przed wyciekami danych.

SKD musi zapewniać odpowiednie mechanizmy zabezpieczające:

- dane osobowe w kopii zapasowej SKD nie mogą być odczytywane przez osoby nieupoważnione,
- kopia bazy danych musi być zaszyfrowana,
- kopia bazy danych musi być zabezpieczona przed możliwością odczytu, importu i przywrócenia na innym serwerze SKD bez kluczy szyfrujących z serwer podstawowego
- SKD musi posiadać dziennik logów, z informacją, kto żąda kluczy szyfrujących, aby przywrócić bazę danych,
- kopia zapasowa SKD może być używana przez serwery redundantne automatycznie bez ograniczeń,
- backup techniczny - Do celów serwisowych musi istnieć możliwość utworzenia kopii zapasowej bez informacji poufnych,

W kontekście RODO procesy systemowe muszą być identyfikowalne z osobą.

Z tego powodu w systemie KD musi istnieć możliwość nadania praw 'super użytkownika' do każdej osoby indywidualnie, która ma posiadać uprawnienia administratora, mając prawo do tworzenia i zarządzania użytkownikami systemu. Super użytkownik musi być identyfikowany z imienia i nazwiska a jego operacje logowane a dzienniku zdarzeń

2.3.4. Neutralność maszyny serwerowej

System KD musi być neutralny względem producenta maszyn serwerowych, centrali głównej tzn.

- system musi posiadać wsparcie dla serwerów fizycznych zgodnych z architekturą 64 bitową,
- spełniać minimalne wymagania parametrów technicznych podanych w karcie katalogowej aplikacji,
- producent systemu KD musi mieć możliwość dostarczenia tylko oprogramowania i licencji.

2.3.5. Wirtualizacja

System KD musi posiadać wsparcie i możliwość instalacji w środowisku wirtualnym.

Minimalne wymagania to wsparcie i możliwość instalacji serwera KD:

- w środowisku Vmware,
- w środowisku Hyper-V.

2.3.6. ACTIVE DIRECTORY AD

System KD musi zapewniać możliwość synchronizacji użytkowników oraz uprawnień z systemem nadrzędnym Active Directory (AD):

- na podstawie informacji z AD dane użytkowników w SKD muszą być aktualizowane automatycznie w ważność ich dostępu odpowiednio modyfikowana,
- aktywacja lub dezaktywacja konta w AD musi powodować odpowiednio przyznanie lub zablokowanie ważności kart w SKD,
- zmiana danych (imienia lub nazwiska) w AD musi zmienić dane powiązanego użytkownika w SKD pozostawiając jednocześnie jego uprawnienia,
- usunięcie użytkownika AD musi spowodować wyłączenie wszystkich kart danej osoby w SKD,
- dodanie nowego użytkownika w AD musi spowodować utworzenie nowej osoby w SKD bez przypisanych kart,
- synchronizacja SKD z AD musi umożliwiać synchronizację uprawnień dostępu do czytników/grupy czytników.

2.3.7. Funkcja redundancji

System KD wymaga funkcji serwera redundantnego, który może działać w trybie cold standby lub hot standby w zależności do konfiguracji na obiekcie. Obie wersje redundancji muszą być dostępne do implementacji. Sposób aktywacji redundancji należy dobrać do warunków panujących na obiekcie.

W przypadku awarii serwera podstawowego i automatycznej aktywacji serwera redundantnego wymagane jest poinformowania operatora o tym, że system działa na serwerze redundantnym.

2.3.8. Dwustopniowe uwierzytelnianie / autoryzacja operatora

System KD musi umożliwiać wszystkim lub wybranym operatorom możliwość dwustopniowej weryfikacji, która ma być dodatkową warstwą bezpieczeństwa.

Weryfikacja z dodatkową warstwą bezpieczeństwa jest potwierdzeniem, że osoby, próbujące uzyskać dostęp do konta są tym, za kogo się podają.

Weryfikacja dwuetapowa zapewnia większe bezpieczeństwo konta operatora systemu KD, ponieważ logowanie obejmuje dwa etapy weryfikacji.

Oprócz hasła trzeba też podać kod wygenerowany przez aplikację na telefonie.

Wymagany schemat działania weryfikacji dwustopniowej:

- najpierw użytkownik musi wprowadzić swoją nazwę użytkownika i hasło. Następnie, zamiast natychmiastowego uzyskania dostępu do interfejsu GUI, użytkownik będzie musiał podać inną dodatkową informację (drugi czynnik),
- druga informacja musi pochodzić z urządzenia/smartfonu operatora z funkcją uwierzytelniania np. aplikacja Google Authenticator lub równoważna,
- wartość drugiego czynnika (kilku cyfrowy numer) musi być losowy i zmieniać się, co kilkanaście, kilkadziesiąt sekund,
- smartphone musi zostać „sparowany” z kontem operatora systemu KD.

2.3.9. Procedury i akcje

System KD musi posiadać moduł procedur, który wywołuje różne akcje.

Procedura to reakcja na pojawiające się zdarzenie (tzw. event) w systemie KD np.: użyto uprawnionej karty, użyto nieuprawnionej karty, użyto nieznanej karty.

Akcja to np. wysłanie wiadomości mail, blokada czytnika, wysterowanie wyjścia.

2.3.10. Procedury - obsługa wyrażeń regularnych w procedurze

System KD musi mieć możliwość wywołanie procedury z filtrowaniem danych w treści zdarzenia za pomocą wyrażeń regularnych.

Przykładowo system KD wyświetlił następujące zdarzenia:

- dostęp do drzwi magazyn przez użytkownika Jan Nowak, nr karty 12345,
- dostęp do drzwi magazyn przez użytkownika Paweł Nowak, nr karty 22345,
- dostęp do drzwi magazyn przez użytkownika Jan Kowalski, nr karty 32345,

System musi mieć możliwość wywołania procedury, gdy w treści zdarzenia znajdują się szukany ciąg znaków np. Jan lub magazyn lub 345.

Muszą być dostępne dwie różne opcje użycia wyrażenia regularnego:

- wyrażenie regularne Posix:
 - ta funkcja wyszukuje, czy wybrane znaki znajdują się gdzieś w ciągu komentarza,
 - często używane klasy wyrażeń regularnych:
 - [abc] dowolne z a, b lub c;
 - [^ abc] nie a, b lub c;
 - [a-g] znak pomiędzy a & g;
 - a* znak zero lub więcej razy;
 - . dowolny znak ;
- Porównanie bez uwzględniania wielkości liter:
 - Ta funkcja wymaga dokładnego dopasowania między ciągiem komentarza a wybranymi znakami, oprócz uwzględniania wielkości liter.

2.3.11. Ilość zdarzeń w bazie SKD

Minimalna liczba zapisywanych zdarzeń w bazie danych kontroli dostępu to co najmniej 10 milionów.

2.3.12. Autoryzacja grupy użytkowników na podstawie lokalizacji stacji roboczej

System KD musi mieć możliwość powiązania możliwości logowania się operatorów z konkretnych lokalizacji fizycznych. W niektórych sytuacjach wymagane jest, aby niektóre stacje robocze miały ograniczone uprawnienia z punktu widzenia bezpieczeństwa.

Wymagane jest, aby pracownika, który pracuje dziś dla działu/lokalizacji A, a jutro dla działu/lokalizacji B miał ograniczona co do rzeczywistego miejsca logowania.

W takim przypadku wymagane jest, aby uprawnienia były określane na podstawie lokalizacji logowania.

Konfigurowalne muszą być:

- uprawnienia do menu, określone przez lokalizację,
- definiowanie uprawnień grupy użytkowników,
- definiowanie typu i lokalizacji stacji roboczej,

W praktyce osoba musi być obecna w obszarze/lokalizacji A, aby się zalogować na stacji roboczej w lokalizacji A. Lokalizacja musi być określona na podstawie strefy KD, czyli wejścia za pomocą imiennej karty zbliżeniowej do lokalizacji A. Jeżeli operator nie będzie według systemu KD obecny w lokalizacji A to autoryzacja na stacji roboczej w lokalizacji A nie będzie możliwa dla tego użytkownika.

2.3.13. Wirtualizacja, ikony widżety i filtry

System KD musi posiadać moduł wizualizacji, gdzie można wyświetlać informacje o systemach oraz sterować systemami.

Z poziomu wizualizacji muszą być między innymi realizowane funkcje:

- KD otworzyć drzwi/czytnik, zamknąć drzwi/czytnik, zablokować czytnik, sprawdzić stan wejść KD i wyjść KD,
- SSWiN za zbroić i rozbroić strefę, zweryfikować stan wejść SSWiN,
- CCTV - podglądać obraz z kamery,
- Interkom - zweryfikować stan połączenia interkomu (aktywna rozmowa),
- wyświetlać widżety z opcją filtrowania danych jak:
 - stan drzwi znajdujących się w trybie Office „biurowym”. Chcesz tylko zobaczyć te drzwi,
 - stan kontrolerów / lokalizacji, które mają problem „usterkę”. Wszystko, co nie ma problemu, nie musi być pokazywane.

2.3.14. Statystyka działania bazy danych

System KD musi posiadać okno wyświetlające statystykę operacji, która działają w bazie danych.

2.3.15. Powiadomienie o wygaśnięciu hasła dla konta operatora

System KD musi posiadać powiadomienie o zbliżającym się terminie wygaśnięcia haseł w formie komunikatu np. „hasło wygasa za x dni”, które będzie widoczne podczas logowania do systemu KD przez operatora. W momencie, gdy pojawi się komunikat o hasle, operator może od razu zmienić hasło.

2.3.16. Automatyczna dystrybucja firmware (Provisioning)

System KD musi posiadać moduł automatycznej dystrybucji oprogramowania układowego (firmware) dla sterowników drzwiowych. Serwer KD musi przysyłać najnowsze oprogramowanie sprzętowe do kontrolera IP, a następnie lokalny kontroler IP musi zapewnić aktualizację wszystkich kontrolowanych przez ten dany kontroler IP sterowników drzwiowych.

2.3.17. Moduł wysyłania transakcji za pomocą wiadomości „push”

System KD musi posiadać wbudowany moduł wysyłanie transakcji (zdarzeń systemu KD) za pomocą wiadomości typu „PUSH” w formacie JSON. Dzięki „usłudze internetowej transakcji push JSON” możliwe jest wysyłanie transakcji systemu KD w formacie JSON do zewnętrznego systemu, takiego jak np. „Elastic Stack” lub innych rozwiązań raportowych, związanych z dashboard.

Moduł musi mieć możliwość precyzyjnego określenia, które transakcje są wysyłane oraz jakie dane są dodawane.

- określając, które typy zdarzeń mają być wysyłane, zapisywane są tylko odpowiednie dane,
- określając, które dane typów zdarzeń mają być wysyłane, zapisywane są tylko odpowiednie dane,
- użytkownik końcowy jest niezależny w wyborze typu bazy danych dla zdarzeń przechowywania,
- użytkownik końcowy jest niezależny przy wyborze rodzaju oprzyrządowania do tworzenia przeglądów/raportów,

2.4. WYMAGANE PROTOKOŁY KOMUNIKACJI

2.4.1. Wsparcie dla protokołu OSDP V2.2

Open Supervised Device Protocol (OSDP) to standard komunikacji kontroli dostępu opracowany przez Security Industry Association (SIA) w celu poprawy współdziałania produktów kontroli dostępu i zabezpieczeń. OSDP został zatwierdzony jako międzynarodowy standard przez Międzynarodową Komisję Elektrotechniczną w maju 2020 roku i został opublikowany jako IEC 60839-11-5.

Projektowany system KD musi posiadać wsparcie do protokołu OSDP w wersji v2.2 (szyfrowanej). System poza obsługą odczytu kart z czytnika musi mieć możliwość konfiguracji długości działania buzzery oraz wejść i wyjść ODSP, które obsługuje czytnik.

OSDP v2.2 z Secure Channel (szyfrowany) musi mieć schemat szyfrowania i uwierzytelniania AES-128 z komunikatami inicjującymi i kluczami, aby zapewnić ścisłą komunikację między zamierzonymi stronami i ukryć dane wymieniane między czytnikiem a kontrolerem.

W przypadku korzystania z protokołu OSDP klucze do odczytu karty znajdują się w samym czytniku kart.

2.4.2. Interpretacja kodowania kart

System KD musi mieć możliwość obsługi różnych typów kodowania kart i interpretacji ich numerów. Za pomocą różnej interpretacji kodowanie kart można używać wielu formatów kart na jednym czytniku, nawet jeśli mają one różną długość danych.

Funkcja ta jest aktywowana, gdy dane przedstawionej karty nie zgadzają się z interpretacją danych powiązaną z czytnikiem. Dane zostaną następnie porównane z innymi interpretacjami danych należącymi do grupy.

Funkcję tę można wykorzystać do łączenia kart DESFire z kartami Mifare UID na jednym czytniku lub kart DESFire z mobilnymi tokenami dostępowymi.

2.5. WYMAGANIA SPRZĘTOWE

2.5.1. Serwer systemu

Charakterystyka:

- napięcie wejściowe 100-240 V AC (50/60 Hz),
- kieszenie dysków 4x3,5" HDD,
- dysk: 1x 2TB SATA 3,5",
- procesor Intel Xeon lub równoważny,
- karta sieciowa 2 x 1GbE LOM,
- pamięć 4 gniazda, DDR4 SDRAM-ECC, DIMM 288-pin, 16GB/128GB maks.,
- montaż U 1U RACK.

2.5.2. Czytnik kart zbliżeniowych

Charakterystyka:

- typ Mifare Classic, Mifare DESFire 0.6, EV1, EV2 oraz EV3,
- częstotliwość 13,56MHz wykrywanie kart,
- zakres temperatury pracy -40°C do 65°C,
- wskaźnik LED, Brzęczyk,
- zgodność z sekcją 889 NDAA,
- interfejs Wiegand, Clock/ Data, RS485,
- stopień ochrony IP55,
- temperatura przechowywania -40°C do 85°C,
- tarty Standard ISO 14443-A, Mifare Classic, Mifare DESFire 0.6, EV1 i EV2,
- dystans czytania kart 20-70mm (w przypadku normalnych operacji),
- zasilanie 5-16V DC, maksymalnie 1,4W.

2.5.3. Sterownik sieciowy

Charakterystyka:

- zasilanie 12 - 24 V DC,
- montaż na szynę DIN 35 mm,
- zgodność z sekcją 889 NDAA,
- szyfrowana komunikacja AES256 między sterownikiem a serwerem,
- system operacyjny LINUX Ubuntu,
- możliwość podłączenia do 4 kontrolerów drzwi w trybie End To End Security (szyfrowanie od karty do serwera),
- temperatura pracy Od -10°C do + 60°C,
- Ethernet Gigabit RJ45.

2.5.4. Kontroler drzwi

Charakterystyka:

- obsługa dwóch przejść jedno lub dwustronnych,
- zgodność z sekcją 889 NDAA,
- wbudowanych 6 wejść monitorowanych,
- temperatura/wilgotność pracy -35°C do +70°C / 20 ~ 90% RH bez kondensacji,
- montaż Szyna DIN 35 mm,
- napięcie zasilania 12 - 24V DC.

2.5.5. Obudowa instalacyjna

Charakterystyka:

- wykonanie z blachy ocynkowanej malowanej w kolorze białym,
- wymiar zewnętrzny 400 mm x 420 mm x 123 mm (SxWxG),
- zamek z kompletem kluczy,
- otwory montażowe do przymocowania do ściany,
- profile montażowe DIN do zamontowania kontrolerów lub sterowników,
- wbudowany kontaktron dla monitoringu otwarcia obudowy oraz oderwania od ściany,
- możliwość obustronnego montażu drzwi,
- otwory wentylacyjne.

2.5.6. Zasilacz

Charakterystyka:

- zasilania 90 - 264 V AC,
- zabezpieczenia: zwarcie / przeciążenie / przepięcie,
- zabezpieczenie przed rozładowaniem akumulatora,
- zabezpieczenie akumulatora przed odwrotną polaryzacją za pomocą bezpiecznika,
- montaż na szynie DIN,
- sygnał alarmowy dla AC OK i akumulatora niski przez styk przekaźnika,
- chłodzenie przez konwekcję swobodnego powietrza,
- wskaźnik LED włączenia zasilania.

3. WYMAGANIA DOTYCZĄCE SPRZĘTU I MASZYN

Wymagania dotyczące sprzętu i maszyn ujęto w **WWiOR-00** "Wymagania ogólne".

4. WYMAGANIA DOTYCZĄCE ŚRODKÓW TRANSPORTU

Wymagania dotyczące środków transportu ujęto w **WWiOR-00** "Wymagania ogólne".

5. WYMAGANIA DOTYCZĄCE WYKONANIA ROBÓT BUDOWLANYCH

5.1. SKŁADOWANIE

Materiały i urządzenia przewidziane do realizacji prac instalacyjnych powinny być składowane zgodnie z zaleceniami producentów.

5.2. PRZYGOTOWANIE DO PRAC MONTAŻOWYCH

Przed rozpoczęciem prac należy zgromadzić wszelkie materiały i urządzenia konieczne do wykonania systemu.

Materiały i urządzenia instalacji przewidziane do montażu powinny być sprawdzone, czy spełniają wymagania DP i właściwej ST. Powinny one posiadać czytelne oznakowanie i być wolne do wad. Nie dopuszcza się montażu materiałów i urządzeń uszkodzonych. W przypadku stwierdzenia uszkodzenia dany materiał lub urządzenie należy wymienić na nowe.

5.3. MONTAŻ URZĄDZEŃ

Montaż urządzeń należy wykonać zgodnie z dokumentacją projektową i wymaganiami podanymi przez producenta.

5.4. PROWADZENIE PRZEWODÓW

Przewody powinny być ułożone zgodnie z projektem.

6. KONTROLA JAKOŚCI

6.1. KONTROLA ZASTOSOWANYCH MATERIAŁÓW

Zgodnie z zapisami **WWiOR-00** "Wymagania ogólne".

6.2. KONTROLA WYKONANYCH ROBÓT

Podczas kontroli jakości wykonanych robót sprawdzeniu podlegać będą:

- zgodność z:
 - dokumentacją projektową (DP),
 - wymaganiami producenta (DTR),
 - zapisami specyfikacji technicznych (ST),
- obecność:
 - kompletnej dokumentacji techniczno-ruchowej (DTR),
 - deklaracje zgodności,
- poprawność wykonania połączeń elementów instalacji,
- usytuowanie urządzeń.

7. PRZEDMIAR I OBMIAR ROBÓT

Zgodnie z zasadami określonymi w **WWiOR-00** "Wymagania ogólne".

8. ODBIÓR ROBÓT

Zgodnie z zasadami określonymi w **WWiOR-00** "Wymagania ogólne".

9. ROZLICZENIE ROBÓT TYMCZASOWYCH I TOWARZYSZĄCYCH

Zgodnie z zasadami określonymi w **WWiOR-00** "Wymagania ogólne".

10. DOKUMENTY ODNIESIENIA

Przez przystąpieniem do realizacji prac Wykonawca musi posiadać znajomość:

- obowiązujących przepisów w zakresie związanym z realizowanymi robotami,
- wymagań producentów dla stosowanych materiałów i urządzeń,
- norm powiązanych w oparciu o które realizowane będą prace.