**FUNKCJONALNOŚĆ SYSTEMU KONTROLI DOSTĘPU W ARESZCIE ŚLEDCZYM**

 **W WARSZAWIE – SŁUŻEWCU**

Projektowany system kontroli dostępu jest systemem skalowalnym i powinien obsługiwać zarówno do obsługi małych instalacji, złożonych z jednego lub kilku przejść, jak i bardzo dużych i rozproszonych terytorialnie. Oprogramowanie zarządzające systemu współpracuje z darmową bazą danych MS SQL Compact lub komercyjną bazą serwerową MC SQL Server. Oprócz podstawowego przeznaczenia jakim jest kontrola dostępu system umożliwia realizację funkcji automatyki budynkowej oraz integracji z innymi systemami np. alarmowymi, systemami telewizji przemysłowej. Aplikacje zarządzające systemem są wykonane w technologii klient-serwer i oferują pracę wielostanowiskową z możliwością definiowania operatorów o różnych poziomach uprawnień.

**Bezpieczeństwo w systemie**

Rozwiązanie powinno oferować wysoki, wielopoziomowy, system bezpieczeństwa, w tym:

• Zastosowanie kart standardu MIFARE z programowalnym numerem zapisanym w szyfrowanych sektorach karty (SSN - Secure Sector Number)

• Obsługa kart MIFARE DESFire i MIFARE Plus oferujących najwyższy poziom bezpieczeństwa

• Złożone tryby logowania wymagające użycia kombinacji Identyfikatorów (np. karta+PIN)

• Komunikacja w sieci LAN/WAN szyfrowana metodą AES128 z dynamicznie zmienianym kluczem szyfrującym (CBC)

• Szyfrowana komunikacja z terminalami dostępu i ekspanderami dołączonymi do magistrali RS485

• Logowanie operatora oprogramowania administracyjnego za pośrednictwem usługi Active Directory

**Ogólna koncepcja systemu**

Podstawowym urządzeniem systemu powinien być strefowy kontroler dostępu. Kontroler powinien umożliwiać obsługę od 2 do 16 przejść dwustronnych. Moduły rozszerzeń oraz czytniki powinny być dołączane do kontrolera za pośrednictwem magistrali komunikacyjnej np. RS485. Magistrala ta powinna umożliwiać tworzenie struktury gwiazdy i mieć długość do 1200m, licząc od kontrolera do najbardziej odległego modułu. Kontroler powinien również współpracować w urządzeniami podłączonymi do sieci komputerowej, poprzez użycie dedykowanego użycie dedykowanego ekspandera, pełniącego rolę interfejsu komunikacyjnego do urządzeń sieciowych.

Przesyłanie ustawień do kontrolerów powinno być realizowane w tle i nie może zatrzymywać bieżącej pracy systemu. Czas przesyłania ustawień nie powinna przekraczać 1 minuty na każdy tysiąc aktywnych użytkowników systemu. Po zakończeniu przesyłania następuje przełączenie systemu na nowe ustawienia, w trakcie, którego system może wstrzymać pracę na kilka sekund. Powinna istnieć możliwość automatycznego synchronizowania ustawień systemu o zadanej porze.

System powinien umożliwiać zarządzanie użytkownikami systemu w trybie online. W trybie tym, aktualizacja danych użytkownika następuje natychmiast po wykonaniu zmian w bazie danych systemu. Zdarzenia zarejestrowane w systemie powinny być na bieżąco pobierane z kontrolerów i zapisywane w bazie danych systemu. Pobierane zdarzeń powinno następować automatycznie przez serwer komunikacyjny systemu i niezależnie od działania zarządzającej systemem. W przypadku braku połączenia z serwerem komunikacyjnym, kontrolery powinny zapisywać zdarzenia w swoich wewnętrznych buforach pamięci.

Wykonanie dowolnej czynności sterującej przez użytkownika systemu może być uwarunkowane posiadaniem właściwego dla danej czynności uprawnienia.

Zasoby sprzętowe kontrolera dostępu mogą być rozszerzane przez dołączanie zewnętrznych modułów i urządzeń. Zewnętrzne zasoby sprzętowe mogą być wykorzystywane wg tych samych zasad, co zasoby płyty głównej kontrolera. Lokalizacja obiektu (linii wejściowej, linii wyjściowej, czytnika itd.), jak i jego rodzaj (typ linii wejściowej, typ linii wyjściowej, typ czytnika) nie powinny mieć wpływu na funkcję logiczną, jaką można powiązać z danym elementem fizycznym.

**Charakterystyka oprogramowania**

**Program narzędziowy**

Programem narzędziowy jest wykorzystywany na etapie instalacji i uruchomienia systemu i służy do konfiguracji niskopoziomowej urządzeń użytych w systemie. Konfigurację niskopoziomową wykonuje się przed instalacją urządzenia.

**Program zarządzający**

Program powinien umożliwiać konfigurowanie logiki systemu oraz jego bieżącą obsługę.

**Baza danych**

System powinien mieć możliwość pracy z serwerową bazą danych MS SQL Server 2016/2022 i nowsze (Express, Business, Enterprise).

W celu zabezpieczenia przed spowolnieniem pracy systemu wskutek dużej ilości danych, baza danych może być automatycznie kompaktowana.

**Praca wielostanowiskowa**

System powinien umożliwiać pracę wielostanowiskowa w architekturze klient-serwer. Ilość stanowisk powinna być nieograniczona.

**Serwer komunikacyjny**

Komunikacja z kontrolerami dostępu powinna być realizowana za pośrednictwem tzw. Serwera komunikacyjnego. Serwer komunikacyjny jako usługa systemu Windows powinien działać niezależnie od aplikacji zarządzającej. Dodatkowo, Serwer komunikacyjny jest odpowiedzialny za realizowanie pewnych globalnych funkcji systemu (Strefy obwodowe, synchronizacja czasu, komendy globalne, automatyczna synchronizacja ustawień o zadanej porze dnia, i inne).

**Operatorzy systemu**

System powinien umożliwiać zarządzanie przez wielu Operatorów o elastycznie kształtowanych uprawnieniach. Program powinien umożliwiać określenie szczegółowych zasad dostępu do większości operacji dostępnych w programie zarządzającym. Logowanie do programu może odbywać się w sposób tradycyjny za pośrednictwem loginu i hasła lub za pośrednictwem usługi Active Directory. W celu ułatwienia zarządzania uprawnieniami Operatorów system powinien umożliwiać zdefiniowanie standardowych typów uprawnień zwanych Rolami. Działania Operatorów systemu powinny być rejestrowane w niezależnym logu, który może być ważnym źródłem informacji w przypadku potrzeby ustalenia charakteru i czasu zmian poczynionych w konfiguracji systemu lub wykonanych operacji sterujących systemem.

**Integracja programowa**

System powinien umożliwiać integrację na drodze programowej za pośrednictwem tzw. Serwera integracji. Serwer integracji jako usługa systemu operacyjnego powinien wykorzystywać technologię WCF, która znacznie redukuje nakład pracy potrzebny na oprogramowanie integracji. Serwer integracji powinien umożliwiać dostęp do bazy danych systemu, zdalne sterowanie systemem oraz zarządzanie jego użytkownikami.

**Program RCP**

RCP jest specjalistycznym programem do analizy i raportowania czasu pracy opracowanym w architekturze klient-serwer. Program taki posiada wiele zaawansowanych funkcji wymaganych przez działy kadrowo-płacowe przedsiębiorstw, w tym funkcje eksportu danych do programów GRATYFIKANT, OPTIMA, SYMFONIA, WF-GANG, TETA. W projektowanym systemie każdy punkt dostępu (czytnik) powinien mieć możliwość wykorzystania jednocześnie do rejestracji czasu pracy. Preferowane do celów rejestracji RCP są terminale wyposażone w wyświetlacz oraz klawisze funkcyjne umożliwiające zmianę rejestrowanego trybu RCP.

Dane wejściowe (m.in. zdarzenia, użytkownicy, grupy) pobierane są automatycznie z bazy danych systemu kontroli dostępu i nie wymagają interwencji osób obsługujących program RCP Master.

RCP może być również wykorzystany poza systemem, ale w takim przypadku dane wejściowe muszą być manualnie importowane z zewnętrznego źródła danych (pliku). Program może być obsługiwany przez operatorów o zróżnicowanych poziomach uprawnień i obsługujących przydzielone do nich grupy pracowników.

**Funkcje systemu**

**Kontrola dostępu do pomieszczeń**

Głównym zadaniem systemu jest realizacja fizycznej kontroli dostępu do stref i pomieszczeń. System powinien być skalowalny i umożliwiać obsługę nieograniczonej ilości przejść. Przejścia mogą być kontrolowane jedno lub dwustronnie. Ilość użytkowników systemu nie powinna być ograniczona. Ograniczeniu podlega ilość identyfikatorów przesyłanych do poszczególnych kontrolerów dostępu. System powinien przesyłać do kontrolera tylko tych użytkowników, którzy posiadają uprawnienie dostępu do przynajmniej jednego przejścia obsługiwanego przez kontroler lub dowolnej z jego funkcji.

**Raportowanie czasu obecności**

System powinien rejestrować zdarzenia związane z ruchem użytkowników na terenie objętym elektroniczną kontrolą dostępu. Rejestr zdarzeń może być wykorzystany do analizy czasu przebywania użytkowników w poszczególnych częściach dozorowanego obiektu. Program zarządzający powinien umożliwiać wyznaczenie czasu przebywania użytkowników w dowolnie zdefiniowanych obszarach systemu (tzw. Strefy obecności) i w dowolnym zakresie czasowym. Raportowanie czasu obecności osób powinno odbywać się przez sumowanie cząstkowych czasów przebywania w określonym obszarze, lub jako czas, który upłynął od momentu pierwszego wejścia aż do momentu ostatniego wyjścia z obszaru w ramach tego samego dnia.

**Rejestracja zdarzeń RCP**

W systemie każdy punkt logowania może być jednocześnie punktem rejestracji czasu pracy (RCP). Rejestracja zdarzenia RCP może następować współbieżnie z przyznaniem dostępu lub być realizowana niezależnie, przez wywołanie dedykowanej do tego celu funkcji. Tryb RCP rejestrowany na danym terminalu może być ustawiony na stałe lub zmieniany przy pomocy wszystkich dostępnych w systemie metod sterowania (harmonogram czasowy, linia wejściowa, klawisz funkcyjny, komenda zdalna). Zmiana trybu RCP terminala może następować na czas nieograniczony, aż do momentu wydania kolejnej komendy, lub wyłącznie na czas wykonania następującej po niej rejestracji RCP. W systemie powinny być dostępne predefiniowane tryby RCP (Wejście, Wyjście, Wyjście służbowe) jak też powinno być możliwe definiowanie własnych trybów dopasowanych do potrzeb konkretnego systemu. Do funkcji terminali RCP najbardziej predestynowane są terminale wyposażone w wyświetlacz i klawisze funkcyjne. Wyświetlacze terminali można skonfigurować do prezentacji bieżącego trybu RCP oraz aktualnego czasu.

**Współpraca z zewnętrznymi programami RCP**

Powinna istnieć możliwość eksportowania zarejestrowanych w systemie do zewnętrznych programów RCP za pośrednictwem pliku wymiany w formacie CSV. W przypadku wykorzystania dedykowanego programu RCP, przekazywanie zdarzeń pomiędzy systemem kontroli dostępu a programem RCP powinno odbywać się automatycznie bez udziału operatora systemu.

**Awaryjne sterowanie przejściem**

System powinien umożliwiać zarówno otwarcie jak i zablokowanie dowolnej grupy przejść w trybie awaryjnym. Tryb ten ma najwyższy priorytet i nie może być zmieniony przez żaden inny dostępny w systemie mechanizm z wyjątkiem dedykowanej do tego celu funkcji kasującej tryb awaryjny. Sterowanie trybem awaryjnym przejścia powinno być realizowane zarówno lokalnie z poziomu urządzeń systemu, jaki i zdalnie z programu zarządzający.

**Rejestracja zdarzeń**

Zdarzenia, które wystąpiły w systemie powinny być na bieżąco ściągane z kontrolerów i zapisywane w bazie danych systemu. Proces ściągania powinien być realizowany przez Serwer komunikacyjny, bez konieczności uruchomienia programu zarządzającego systemem. W przypadku, gdy połączenie z kontrolerem jest nieosiągalne zdarzenia powinny być rejestrowane w wewnętrznym buforze zdarzeń kontrolera i pobierane automatycznie po przywróceniu komunikacji.

**Powiadamianie o wystąpieniu zdarzenia**

System powinien umożliwiać zdefiniowanie powiadomienia, które ma być wyświetlone na ekranie monitora lub wiadomości email, która ma być wysłana w momencie wystąpienia konkretnego zdarzenia. Korzystając z uniwersalnego mechanizmu filtru zdarzeń można dodatkowo określić inne warunki (m.in. czas i miejsce wystąpienia zdarzenia), które muszą wystąpić, aby system wykonał akcję przypisaną do danego rodzaju zdarzenia.

**Monitorowanie zdarzeń**

Zdarzenia, które wystąpiły w systemie powinny być na bieżąco wyświetlane w oknach Monitorowania online. Każde z okien może być skonfigurowane do wyświetlania wybranej grupy zdarzeń i dokowane na dodatkowych monitorach.

**Monitorowanie obecności**

System powinien umożliwiać monitorowanie osób zalogowanych w dowolnie zdefiniowanym obszarze systemu. Powinno być możliwe monitorowanie wielu obszarów jednocześnie. W szczególnym przypadku monitor obecności może być użyty w celu prezentacji listy osób, które zarejestrowały się na wybranym punkcie dostępu w następstwie ogłoszenia ewakuacji budynku.

**Monitorowanie przejść**

System powinien umożliwiać monitorowanie wybranych przejść i podgląd zdarzeń, które na nich wystąpiły. W momencie wystąpienia zdarzenia system powinien automatycznie wyświetlić podgląd z kamery CCTV skojarzonej z miejscem wystąpienia zdarzenia lub zdjęcie osoby, która została zarejestrowana na tym miejscu.

**Monitorowanie statusu RCP**

System powinien umożliwiać wyświetlanie na bieżąco listę osób zalogowanych w dowolnym obszarze systemu wraz ze wskazaniem ich aktualnego statusu RCP, który wskazuje, jaki typ obecności jest w danej chwili rejestrowany na konto danego użytkownika systemu.

**Mapy**

W systemie powinna być możliwość definiowania Mapy bazujących na dowolnych podkładach graficznych i nanoszenie na nie w procesie konfiguracji symbole reprezentującego wybrane elementy systemu (m.in. Przejścia, Punkty logowania, kamery CCTV). Z poziomu widoku Mapy powinna być możliwość wywołania podglądu na żywo z kamery skojarzonej z danym symbolem jak też wykonanie komendy zdalnej.

**Kontrola liczby osób w strefie**

System powinien umożliwiać kontrolę liczby osób zalogowanych w strefie dostępu oraz określenie limitu dolnego oraz górnego liczby osób, które mogą przebywać w strefie.

**Funkcja Anti-passback (APB)**

Funkcją APB powinna umożliwiać objęcie zarówno pojedyncze pomieszczenie kontrolowane przez przejście dwustronnie, jak i obszaru kontrolowanego przez wiele przejść z punktami wejścia i wyjścia ze strefy. W przypadku naruszenia zasad APB system może blokować dostęp lub ograniczyć się do rejestracji odpowiedniego zdarzenia. System udostępnia również funkcję czasowego APB (T-APB), która dopuszcza do ponownego wejścia do pomieszczenia lub strefy o ile od momentu wejścia upłynęło wystarczająco dużo czasu zdefiniowanego w zastawach systemu. W przypadku zastosowania funkcji T-APB możliwe jest stosowanie funkcji APB również na przejściach jednostronnych. W większości przypadków, szczególnie na przejściach z rejestracją RCP, stosowanie funkcji T-APB jest wystarczająco skutecznym sposobem blokady przed próbami uzyskania dostępu przez użyczenie identyfikatora osobie trzeciej. W odróżnieniu od standardowej logiki działania funkcji APB, funkcja T-APB nie wymusza instalacji terminali dostępu rejestrujących opuszczenie pomieszczenia lub strefy a dodatkowo znacznie ułatwia użytkownikom systemu, którzy nie są karani blokadą dostępu w przypadku, gdy opuszczenie pomieszczenia lub strefy nastąpiło z pominięciem terminala wyjściowego. Stosowanie T-APB może być stosowane również gdy w systemie są zainstalowane terminale wyjściowe ale w tym przypadku, ponowne wejście do strefy może nastąpić w dowolnie krótkim czasie po jej opuszczeniu przez terminal wyjściowy lub po predefiniowanym czasie określonym dla funkcji T-APB.

**Weryfikacja otwarcia drzwi**

System powinien udostępniać opcję, która uzależnia decyzję o zmianie miejsca, w którym przebywa użytkownik od tego czy po przyznaniu dostępu nastąpiło otwarcie drzwi. Jeśli drzwi nie zostały otwarte system uznaje, że użytkownik nie zmienił miejsca przebywania.

**Blokowanie ruchu z pominięciem terminali dostępu**

System powinien umożliwiać blokowanie możliwości przejść pomiędzy strefami, które ze sobą nie sąsiadują. Funkcjonalność ta ma na celu przeciwdziałanie poruszaniu się z pominięciem urządzeń kontroli dostępu i umożliwia tworzenie tzw. Ścieżek dostępu.

**Obsługa przejść typu Śluza**

System powinien umożliwiać tworzenie stref złożonych z dwóch lub więcej przejść, w których obowiązuje zasada, że tylko jedno przejście w danej chwili może być otwarte.

**Obsługa przejść dwustronnych**

System powinien umożliwiać realizację przejść dwustronnych, w których istnieje potrzeba rozróżnienia kierunku dostępu.

**Harmonogramy**

Harmonogramy umożliwiają uzależnienie działania systemu od konkretnego dnia tygodnia i pory dnia. Harmonogramy mogą być wykorzystane przy konfigurowaniu działania wielu funkcji systemu, a w szczególności uprawnień dostępu.

**Kalendarze**

Kalendarze są wykorzystywane do zmiany logiki systemu w okresach świątecznych lub urlopowych - w szczególności do zmiany uprawnień dostępu. Kalendarze powinny obejmować okres wielu lat.

**Uprawnienia**

W systemie wykonanie dowolnej akcji lub funkcji powinno być uwarunkowane wymogiem posiadania właściwego Uprawnienia. Uprawnienie określa, kiedy i gdzie dana akcja (funkcja) może być wykonana. Uprawnienia powinny być przypisywane bezpośrednio do Identyfikatora, Użytkownika lub Grupy użytkowników. Uprawnienia przypisane do Grupy dostępu przechodzą automatycznie na wszystkich Użytkowników należących do danej Grupy. Uprawnienia przypisane do Identyfikatora automatycznie przechodzą na Użytkownika, do którego dany Identyfikator należy.

**Uprawnienia do dostępu**

W mniejszych systemach wygodniejsze jest definiowanie uprawnień dostępu osobno dla każdego Punktu logowania. W dużych obiektach bardziej korzystne jest definiowanie prawa dostępu w odniesieniu do obszarów złożonych z wielu Punktów logowania (tzw. Stref dostępu). W projektowanym systemie powinny być dostępne obydwa te warianty definiowania uprawnień.

**Strefy dostępu**

Strefy dostępu umożliwiają podział systemu na obszary złożone z wielu przejść, co w przypadku większych systemów jest ułatwieniem przy zarządzaniu uprawnieniami dostępu. Dodatkowo, logika Stref dostępu powinna umożliwiać kontrolę liczby osób przebywających w strefie a także stosowanie funkcji APB.

**Strefy obwodowe**

System powinien umożliwiać definiowanie obszarów, wewnątrz których przemieszczanie się jest możliwe tylko wtedy, gdy użytkownik wcześniej zalogował się na wyznaczonym punkcie kontrolnym. Zwykle, punktem takim jest czytnik zamontowany na wejściu do budynku, natomiast czytniki wewnątrz budynku są jej punktami wewnętrznymi. Funkcjonalność Stref obwodowych powinna być realizowana przez Serwer komunikacyjny systemu. Strefy obwodowe mogą obejmować obszary będące pod kontrolą wielu kontrolerów dostępu.

**Progi dostępu**

Użytkownik może uzyskać dostęp na danym Punkcie logowania, jeśli Próg dostępu przypisany do Identyfikatora, którego użył nie jest niższy od Progu dostępu ustawionego na danym Punkcie logowania. Próg dostępu może być wykorzystany, jako dodatkowy element logiki kształtującej prawa dostępu w obiekcie. W przypadku prostych systemów wykorzystanie Progów dostępu może zastępować potrzebę definiowania Uprawnień poprzez zdefiniowanie hierarchicznej struktury progów dostępu, w której każdy wyższy próg obejmuje część (podzbiór) Punktów dostępu wchodzących w skład poprzedniego Progu dostępu.

**Użytkownicy**

W systemie rozróżniane są trzy typy Użytkowników:

• Osoby

• Goście

• Wyposażenie

Każdy Użytkownik systemu może posiadać jeden lub więcej Identyfikatorów. Dane skasowanych Użytkowników systemu nie ulegają zatarciu i mogą być odtworzone w dowolnym momencie.

**Osoby**

Osoby są Użytkownikami systemu, których obecność w systemie nie jest ograniczona czasowo. System powinien udostępniać szeroki zakres danych opisujących Osobę. Powinna również Istnieć możliwość tworzenia własnych parametrów (tzw. Pól użytkownika) rozszerzających sposób opisywania Osób. System powinien zapewniać zgodność z prawodawstwem związanym z wymogiem ochrony danych osobowych. Osoby mogą być członkami Grup. Grupy mogą tworzyć struktury hierarchiczne. Uprawnienia Osoby są sumą Uprawnień przypisanych do posiadanych przez nią Identyfikatorów, Uprawnień własnych oraz uprawnień dziedziczonych z Grup, do których dana Osoba należy.

**Goście**

Goście są Użytkownikami systemu, których tworzy się na okoliczność wizyty i którym można przydzielić Opiekuna. System powinien automatycznie blokować możliwość poruszania się Gościa poza przedziałem czasowym określonym przez datę i godzinę początku oraz końca wizyty. Goście powinni być monitorowani w osobnym oknie zdarzeń poprzez wybór odpowiedniego filtra wyświetlającego zdarzenia związane z pobytem Gościa w obiekcie.

**Wyposażenie**

Wyposażenie jest kategorią nieosobowych Użytkowników systemu, która odnosi się do przedmiotów, wobec których istnieje wymóg kontroli i rejestracji ruchu. Typowo, wymóg taki może występować wobec samochodów, kluczy lub wartościowych przedmiotów. Do Wyposażenia można przypisać Identyfikator oraz Uprawnienia oraz powiązać je z Osobą, która jest jego właścicielem lub dysponentem.

**Identyfikatory**

System powinien pracować z wieloma typami Identyfikatorów jednocześnie. Każdy Użytkownik systemu powinien mieć możliwość posiadania wiele, różnego typu Identyfikatorów. Identyfikatory powinny być wczytywane do systemu z poziomu dowolnego czytnika systemowego lub dedykowanego czytnika administratora podłączonego do portu USB komputera. Karty można wprowadzić do systemu z wyprzedzeniem i przechowywać je w tzw. Zasobniku. W przypadku pracy z kartami MIFARE powinno być możliwe programowanie numerów kart w momencie ich wprowadzania do systemu.

**Programowanie kart**

System powinien umożliwiać programowanie kart MIFARE za pośrednictwem czytnika administratora.

**Seryjne wprowadzanie kart**

System powinien umożliwiać seryjne wprowadzanie kart. W celu wprowadzenia wielu kart należy podać kod pierwszej karty oraz ilość kart do wprowadzenia. Kolejne karty powinny być wprowadzane automatycznie z kodem różniącym się o jedność względem karty poprzedniej.

**Sposoby wyzwalania akcji w systemie**

System powinien oferować kilkadziesiąt funkcji, które określają sposób reakcji systemu na określone sytuacje. Wyzwolenie funkcji może następować za pośrednictwem następujących metod:

• Z linii wejściowej

• Z klawisza funkcyjnego

• Poprzez logowanie użytkownika na czytniku

• Zdalnie z poziomu programu zarządzającego

Wyzwolenie akcji w systemie powinno być związane z wymogiem logowania użytkownika wywołującego akcję oraz posiadaniem przez niego odpowiedniego Uprawnienia.

**Wyzwalanie akcji przez logowanie**

Logowanie użytkownika powinno umożliwiać automatycznie wywoływać wykonanie funkcji. System rozróżnia następujące formy logowania Użytkownika:

• Normalne

• Specjalne

• Podwójne

• Włożenie karty do kieszeni

• Wyjęcie karty z kieszeni

Każda z form logowania powinna umożliwiać wywoływanie innej funkcji. Konfigurowanie funkcji wywoływanej przez konkretny typ logowania powinno być realizowane indywidualnie dla każdego Punktu logowania. Najczęściej, logowanie Normalne jest wykorzystywane w celu uzyskania dostępu, natomiast logowanie specjalne, do zmiany stanu systemu alarmowego lub sterownia automatyką budynku.

**Komendy zdalne**

Oprogramowanie systemu powinno umożliwiać wykonanie dowolnej funkcji systemu z poziomu programu zarządzającego. Komendy zdalne mogą dotyczyć dowolnej części systemu. Aby Operator programu mógł wykonywać zdalnie komendę musi on być jednocześnie Użytkownikiem systemu i posiadać Uprawnienie do funkcji, która ma być wykonana. Komendy zdalne powinny być wywoływana zarówno z poziomu widoków obiektów konfiguracyjnych systemu (Przejścia, Punkty automatyki, Strefy Dostępu, Strefy alarmowe itd.) jak i z poziomu widoku Map.

**Komendy globalne**

System powinien umożliwiać wykonanie wielu funkcji w wielu miejscach systemu jednocześnie poprzez wywołanie tzw. Komendy globalnej. Komenda globalna może być wywołana na żądanie operatora systemu, automatycznie wg zdefiniowanego harmonogramu, w reakcji na wystąpienie określonego zdarzenia w systemie lub z poziomu serwera integracji. Jednym z typowych sposobów wykorzystania Komend globalnych jest otwarcie lub zablokowanie awaryjne wszystkich przejść w systemie przez użycie jednego z kilku zdefiniowanych w systemie przycisków awaryjnych. Komedy globalne powinny być wykonywane przez Serwer komunikacyjny systemu.

**Wielofunkcyjne linie wejściowe**

Linie wejściowe mogą być konfigurowane do dowolnych funkcji niezależnie od miejsca (urządzenia), na którym się fizycznie znajdują. Do linii wejściowej można przypisać wiele funkcji jednocześnie, funkcje te mogą wywoływać reakcję w różnych miejscach systemu. Typowym przykładem wykorzystania wielofunkcyjności jest awaryjne otwarcie wielu drzwi z poziomu jednego przycisku podłączonego do dowolnie wybranej linii wejściowej.

**Wielofunkcyjne linie wyjściowe**

Linie wyjściowe mogą być konfigurowane do dowolnych funkcji niezależnie od miejsca (urządzenia), na którym się znajdują. Linia wyjściowa może być skonfigurowana do wielu funkcji jednocześnie. W przypadku jednoczesnego wystąpienia dwóch lub więcej funkcji, wyjście jest sterowane przez funkcję o najwyższym priorytecie. Sposób sterowania wyjściem powinien być indywidualnie definiowany dla każdej z przypisanych do wyjścia funkcji. Sterowanie wyjściem powinno następować w sposób statyczny (załącz/wyłącz) lub modulowany wg indywidualnie zdefiniowanego wzorca.

**Wejścia Dual Wiring**

Większość urządzeń systemu powinno oferować parametryczne linie wejściowe, które mogą być między innymi skonfigurowane do typu Dual Wiring. Wejścia tego typu umożliwiają obsługę dwóch różnych źródeł sygnałów (np. przycisków). Rozróżnienie źródła wyzwolenia następuje przez pomiar wartości rezystancji włączonej w obwód źródła sygnału wejściowego.

**Technologie identyfikacji**

W ramach tego samego systemu dostępu powinna być możliwość stosowania identyfikatorów wykonanych w różnych technologiach. Użytkownik systemu może posiadać i stosować współbieżnie karty MIFARE, EM, identyfikatory mobile (Bluetooth, NFC), różne formy identyfikacji biometrycznej (linie papilarne, skanery naczyń, owalu twarzy, źrenicy oka itd.) hasła alfanumeryczne i inne. Odczyt poszczególnych typów identyfikatorów może być realizowany na osobnych czytnikach, które zostały zainstalowane w ramach jednego Punktu logowania.

**URZĄDZENIA SYSTEMU**

**ZESTAW KONTROLI 4 PRZEJSĆ**

Zestaw kontroli dostępu przeznaczony do obsługi czterech przejść w systemie. W skład zestawu wchodzi metalowa obudowa z zasilaczem, sieciowy kontroler dostępu i ekspander we/wy. Zestaw umożliwia obsługę czterech przejść dwustronnych z wykorzystaniem czytników RS485. Każde przejście jest obsługiwane przez niezależny zestaw wyjść zasilających złożonych z wyjścia 0,2 A do zasilania czytników i wyjścia 1,0 A do zasilania zamka lub przekaźników sterujących zamkami oraz pozostałych elementów przejścia. Prąd ładowania akumulatora może być ustawiony na wartość 0,3 A, 0,6 A lub 0,9 A. Zestaw umożliwia kompletne zasilenie wszystkich kontrolowanych przejść.

**Charakterystyka:**

• zestaw kontroli dostępu dla 4 przejść
• obustronna kontrola przejścia
• sieciowy kontroler dostępu
• ekspander we/wy
• obsługa czytników RS485 (16 czytników)
• obsługa czytników z interfejsem OSDP (16 czytników, wymagany dodatkowy interfejs)

• 4 wyjścia zasilania 0,2 A
• 4 wyjścia zasilania 1,0 A
• 0,3 A/0,6 A/0,9 A prąd ładowania akumulatora
• zabezpieczenie przed głębokim rozładowaniem
• łącznik antysabotażowy
• miejsce na akumulator 17 Ah
• zasilacz sieciowy 13,8 V/6 A

**CZYTNIKI KART ZBLIŻENIOWYCH**

Czytniki są zewnętrznymi terminalami dostępu przeznaczonymi do pracy w systemie kontroli dostępu. Czytniki pełnią funkcję urządzenia podrzędnego względem kontrolera dostępu i nie mogą samodzielnie dozorować przejścia. Terminale umożliwiają zarówno odczyt numeru seryjnego karty zbliżeniowej (CSN) jaki i numeru programowalnego (PCN) zapisanego w szyfrowanych sektorach pamięci na karcie. Wykorzystanie programowalnego numeru karty zabezpiecza ją przed duplikowaniem co zdecydowanie podnosi poziom bezpieczeństwa całego systemu kontroli dostępu. W obiektach wymagających najwyższego poziomu bezpieczeństwa należy stosować karty MIFARE DESFire EV1 oraz MIFARE Plus.

Charakterystyka

karty zbliżeniowe ISO14443A, odczyt numeru seryjnego karty (CSN):

-- MIFARE Ultralight

-- MIFARE Classic 1k oraz 4k

-- MIFARE Plus

-- MIFARE DESFire EV1

• odczyt numeru programowalnego karty (PCN):

-- MIFARE Classic 1k oraz 4k

-- MIFARE Plus

-- MIFARE DESFire EV1

• zasięg odczytu do 7 cm (karty Ultralight i Classic)

• zasięg odczytu do 3 cm (karty DESFire i Plus)

• rozpoznawanie długiego przyłożenia karty

• interfejs komunikacyjny RS485

• trzy wskaźniki LED

• trzy wejścia parametryczne

• czas reakcji wejść definiowany w zakresie od 50 do 5000 ms

• możliwość pracy wejść w trybie Double Wiring

• wyjście przekaźnikowe 1,5 A/30 V

• dwa wyjścia tranzystorowe 150 mA/15 V

• definiowanie polaryzacji spoczynkowej linii wyjściowej

• głośnik sygnalizacyjny z regulowanym poziomem dźwięku

• klawiatura z regulowanym poziomem podświetlenia

• detekcja otwarcia obudowy oraz oderwania od podłoża

• zasilanie 12 VDC

• konfiguracja przez RS485

• aktualizacja oprogramowania wbudowanego przez RS485

• praca w warunkach zewnętrznych

• wymiary (wys. x szer. x grub.):

-- podstawa standardowa: 152,5 x 46,0 x 23,0 mm

-- podstawa wysoka: 152,5 x 46,0 x 35,0 mm

• znak CE

**CZYTNIK ADMINISTRATORA**

Czytnik i programator transponderów zbliżeniowych standardu 13,56MHz ISO/IEC 14443A MIFARE Classic oraz MIFARE DESFire EV1 z funkcją odczytu kodów kart EM 125 kHz. Zasilany jest z portu szeregowego USB który jest także wykorzystywany do komunikacji z urządzeniem. Czytnik posiada stabilną nabiurkową obudowę metalową z uchwytem na kartę Czytnik znajduje zastosowanie, jako uniwersalny czytnik numerów kart, jak również pozwala na wygodne wprowadzanie identyfikatorów użytkowników w systemach kontroli dostępu. Funkcję programowania transponderów MIFARE Classic i DESFire udostępniono w programie narzędziowym. Dla programistów chcących zintegrować obsługę tego urządzenia w innych aplikacjach dostępny jest pakiet deweloperski SDK.

Charakterystyka:

• zasilanie 5 VDC bezpośrednio z portu USB

• średni pobór prądu 80 mA

• karty MIFARE Classic, EM 125 kHz

• karty MIFARE DESFire (tylko RUD-4-DES)

• zasięg odczytu kart MIFARE Classic do 3 cm

• zasięg odczytu kart EM 125 kHz do 4 cm

• zasięg odczytu kart MIFARE DESFire do 2 cm (tylko RUD-4-DES)

• przekaźnik NO/NC; 1 A/30 V

• czas odczytu ok. 200 ms

• konfiguracja z komputera PC

• praca w warunkach wewnętrznych

• pakiet SDK

• warunki pracy:

-- temperatura: od +5°C do +45°C

-- wilgotność: od 0% do 95%

• znak CE

**ZWORA ELEKTOMAGNETYCZNA**

* Maks. nacisk na drzwi powyżej 500 kg
* Przeznaczenie Wewnętrzna
* Napięcie zasilania 12V DC / 24V DC
* Pobór prądu 600mA (12V DC) / 300mA (24V DC)
* Sygnalizacja styk NO/NC, czujnik hallotronowy
* Dioda informacyjna LED Tak
* Wymiary zwory (szer. x wys. x gł.) 265 x 76 x 41 mm
* Wymiary płytki (szer. x wys. x gł.) 185 x 60 x 13,5 mm

**ZAMEK ELEKTRYCZNY**

Zamek elektryczny bębnowy do drzwi przejściowych. Zastosowanie wysokogatunkowych materiałów do konstrukcji zamka zapewnia bezawaryjną pracę wewnątrz i na zewnątrz budynków. Zainstalowane w zamku czujniki dają pełną informację o stanie zamknięcia. Sterowanie elektromechaniczne oraz klucz. Zamek (element montowany w futrynie oraz na kracie) należy zamontować (wspawać) ze starannością oraz estetyką jak i zabezpieczyć wykonane spawy przed korozją.

* Napięcie stałe 24V, prąd 0,9A lub wersja napięcie stałe 12V, prąd 1.6A
* Wymiary (szerokość x wysokość x głębokość) w milimetrach: 61 x 156 x 182
* Norma **PN-EN 14846:2010** klasyfikacja końcowa wyrobu: **3A5000710**
* Norma **PN-EN 12209:2016-04** klasyfikacja końcowa wyrobu: **3A50007**

**LAMPKA SYGNALIZACYJNA**

Sygnalizator optyczny przeznaczony do montażu wewnątrz budynków. Należy zamontować go nad kratą w widocznym miejscu w pozycji poziomej tak aby sygnalizacja otwarcia była widoczna z obu stron przejścia. Do wyboru dostępny jest jeden z czterech rodzajów sygnalizacji realizowanej przez zespół jasnych diod LED (ciągłe świecenie, szybkie miganie, wolne miganie oraz dwa błyski, po których następuje sekundowa przerwa).

* Napięcie zasilania (±15%) 12 V DC
* Wymiary obudowy ø97 x 37 mm
* Zakres temperatur pracy -10…+55 °C
* Maksymalny pobór prądu 44 mA

**KLUCZ LICENCYJNY**

Sprzętowy klucz licencyjny podłączany do sieci komputerowej, w której funkcjonuje licencjonowane oprogramowanie.

Komunikacja z kluczem szyfrowana jest metodą AES128b CBC EtM. RLK-1 zwykle jest wykorzystywany w przypadku instalacji licencjonowanego oprogramowania na wirtualnych maszynach. Urządzenie umieszczone jest w obudowie montowanej na szynie DIN.

* napięcie zasilania: 12 VDC
* średni pobór prądu: ~ 125 mA
* Ethernet 10/100 Mb
* interfejs RS485
* szyfrowanie AES128b CBC EtM
* klasa środowiskowa I (wg EN 50131-1):
	+ warunki wewnętrzne
	+ temp. +5°C do +40°C
	+ wilgotność względna 10…95% (bez kondensacji)
* IP 20
* wymiary: 62,0 × 73,0 x 85,0 mm  (szer. x wys. x gł.)
* waga: ~ 110 g
* CE, RoHS

**SERWER**

Serwer należy zamontować w serwerowni budynku administracyjnego na parterze oraz wykorzystać istniejące połączenie światłowodowe.

 Typ obudowy: Obudowa serwerowa Rack 2U

Standard płyty głównej: Micro ATX

Procesor: Intel Core i7-13700K, 3.4 GHz,

Rdzenie / wątki: 8P/8E/24W

Taktowanie: 3.4 GHz

Taktowanie turbo: 5.4 GHz

Cache: 30 MB

Typ karty graficznej: Zintegrowana Intel UHD Graphics 770

Pamięć RAM: 64 GB, 5200MHz, DDR5 (do 192GB)

Gniazda pamięci ogółem / zajęte: 4/2 & 4/1

Dysk: 250GB, SSD M.2 PCI-E (2szt. – RAID 1)

Prędkość odczytu/zapisu danych: 2900 MB/s / 1300 MB/s

Komunikacja:

Iość portów Ethernet LAN (RJ-45) 3 porty: 2 - 2.5 Gigabit Ethernet, 1 - Gigabit Ethernet

Złącza zewnętrzne: -2 x USB 3.2 Gen 2 ports (1 x Type-A, 1 x Type-C®) -4 x USB 3.2 Gen 1 ports (4 x Type-A) -1 x DisplayPort -1 x HDMI® port -1 x VGA port from AST2600 -2 x Intel® 2.5Gb Ethernet ports -1 x Realtek 1Gb Ethernet dedicated for AST2600 -3 x Audio jacks -1 x BIOS FlashbackTM button

- PS/2 klawiatura/mysz – 1szt.

Obsługa RAID RAID 0 / RAID 1 / RAID 5 / RAID 10 / RAID 50 / RAID 60 / JBOD

Zasilacz: 600W

System operacyjny: Microsoft Windows 11 Pro PL 64 bit

Wymiary obudowy: 89 x 481 x 688 mm

Gwarancja: 24 miesiące

**STACJA KLIENCKA**

* Typ obudowy: Middle/Midi Tower
* Standard płyty głównej: mATX, ATX
* Procesor: Intel Core i5
* Rdzenie / wątki: 6/12
* Taktowanie: 3.6 GHz
* Taktowanie turbo: 5.0 GHz
* Typ karty graficznej: Dedykowana
* Pamięć VRAM: 2/4 - GB GDDR6
* Pamięć RAM: 16 GB, 3200MHz, DDR4
* Gniazda pamięci ogółem / zajęte: 4 / 2
* Dysk: 512 GB, SSD M.2 PCI-E
* Prędkość odczytu/zapisu danych: nie mniejsza niż 3000 MB/s / 2000 MB/s
* Komunikacja: LAN 2.5G Ethernet (10/100/1000/2500 Mbps) - zintegrowana
* LAN 1G Ethernet (10/100/1000 Mbps) - dedykowana
* Złącza zewnętrzne: DisplayPort x1, HDMI x1, PS/2 (klawiatura/mysz) x1, RJ-45 x1, USB 2.0 x4,
USB 3.2 Gen 2 (3.1 Gen 2) x2, Złącze audio x3 RJ-45 (Ethernet) – dodatkowa karta sieciowa
* Obsługa RAID RAID 0 / RAID 1 / RAID 5 / RAID 10
* Złącza karty graficznej: 1x HDMI 2.0b 1x DisplayPort 1.4a 1x DVI
* Zasilacz: moc niemniejsza niż 700W
* System operacyjny: Microsoft Windows 10/11 Professional PL
* Wymiary obudowy: 450mm x 232mm x 463mm (dł. x szer. x wys)
* Gwarancja: 24 miesiące
* Dodatkowe wyposażenie: Przewód zasilający, instrukcje obsługi podzespołów, klawiatura + mysz.

**MONITOR (do stacji klienckiej)**

* Przekątna ekranu: minimum 30”
* Proporcje ekranu: 16:9
* Rozdzielczość: 1920 x 1080
* Czas reakcji matrycy: 5 ms
* Jasność: 250 cd/m2
* Kontrast: 20000000:1 (DCR)
* Wejście: 1xHDMI, 1xVGA, 1x CVBS
* Zabezpieczenia: Kensington Security Slot™
* Czas pracy: 24/7
* Temperatura pracy: -20...60 °C

**KOMPUTER WRAZ Z MONITOREM (obsługa systemu z pozycji administratora)**

 W celu obsługi systemu z pozycji administratora oraz uprawnionego użytkownika do programowania kart jak i nadawania uprawnień użytkowników należy dostarczyć oprogramowanie, które będzie zainstalowane na komputerze dostarczonym przez zamawiającego.

**ILOŚĆ PRZEJŚĆ ORAZ RODZAJU ZASTOSOWEGO ZAMKA**

* 12 przejść – Zamek elektryczny do krat przejściowych (sygnalizacja optyczna nad kratą)
* 2 przejścia – zwora elektromagnetyczna (bez sygnalizacji optycznej)

Do 13 przejść należy zastosować czytnik dwustronny oraz w przypadku wejścia do serwerowni jednostronny z wewnętrznym przyciskiem wyjścia;

Do wszystkich przejść należy zamontować samodomykacz.

**OKABLOWANIE**

Do każdego przejścia zostało ułożone okablowanie do czytników 2x skrętka kat. 6, lampki sygnalizacyjnej i kontaktronu 1x skrętka kat. 6 oraz zamka 1x przewód okrągły giętki linka H05VV-F 3Gx1,5mm2