Załącznik nr 6 do SIWZ

**Specyfikacja techniczna i funkcjonalna**

## **Założenia ogólne**

Celem instalacji systemu jest umożliwienie kontroli dostępu do pomieszczeń w budynkach uczelni:

* A – Budynek Główny (łącznie ze skrzydłem i Pawilonem),
* B – Budynek Banku,
* C – Budynek Towarowa,
* D – Budynek Collegium Altum,
* E – Budynek SPNJO,
* DS. Atol (łącznie z budynkiem „Archiwum”),
* DS. Dewizka,
* DS. Feniks,
* SWFiS,

przy wykorzystaniu dedykowanych kart lub legitymacji pracowniczych i studenckich.

Zestawienie i specyfikacja typów przejść objętych zamówieniem znajduje się w załączniku nr 7 do SIWZ Zestawienie przejść, gdzie zawarto informacje dotyczące między innymi:

1. oznaczenia przejścia,
2. rodzaju blokady (elektrozaczep, zwora elektromagnetyczna itp.),
3. rodzaju przejścia (jednostronne – czytnik i przycisk lub dwustronne dwa czytniki itp.),
4. zaleceń ppoż (przycisk ewakuacyjny itp.)
5. zaleceń montażowych (wymiana klamki na gałkę itp.).

W przypadku przejść online przewodowych i wskazanych przejść bezprzewodowych, należy uwzględnić możliwość ewentualnego podłączenia w przyszłości do systemu czujnika umożliwiającego stałe monitorowanie stanu otwarcia/zamknięcia drzwi (kontaktronu).

Podczas instalacji, stosując się do przepisów ppoż, dla wymaganych przejść należy zainstalować odpowiednie przewody umożliwiające integrację systemu z istniejącymi w poszczególnych budynkach centralami ppoż., tak aby w przypadku pożaru drzwi zostały automatycznie odblokowane.

Instalowany system kontroli dostępu powinien umożliwiać zarządzanie, konfigurację, raportowanie zdarzeń itp.

W zakresie prac należy uwzględnić dostarczenie i wgranie obiektów SIO na kartę typu MIFARE (13,56MHz) na używanych przez Zamawiającego kartach (300 szt.).

Oprogramowanie obsługujące system docelowo powinno odpowiadać założeniom dla kategorii PSIM (Physical Security Information Management) umożliwiając integrację różnych systemów bezpieczeństwa. Kluczowe zagadnienia to:

1. Zarządzanie, gromadzenie i przetwarzanie danych z różnych systemów bezpieczeństwa (np. kontrola dostępu, monitoring, system obsługi dostępu do parkingów w oparciu o karty UHF oraz odczytywane numery rejestracyjne pojazdów).
2. Analiza i powiązanie kluczowych z punktu widzenia bezpieczeństwa danych o zaistniałych zdarzeniach umożliwiające szybką klasyfikację incydentu.
3. Przygotowanie procedur dla operatorów umożliwiających przejście procesu związanego z incydentem.
4. Rozbudowane raportowanie na temat zaistniałych incydentów/zdarzeń oraz działań przeprowadzanych przez operatorów i administratorów systemu.

## **Projekt**

Przed przystąpieniem do prac instalacyjnych w danym budynku, należy wykonać projekt instalacyjny obejmujący m.in. następujące zagadnienia:

1. Liczbę i lokalizację kontrolerów i innych niezbędnych do prawidłowego funkcjonowania systemu urządzeń, we wskazanych węzłach sieci komputerowej oraz przyporządkowanie każdego przejścia do konkretnego węzła/kontrolera systemu. Instalację urządzeń z uwzględnieniem minimalizacji potrzebnego do instalacji miejsca (np. instalacja kilku urządzeń w jednej obudowie z dedykowanymi zasilaczami – akumulatorami i transformatorem).
2. Odpowiednie przypisanie poszczególnych przejść do urządzeń i lokalizacji.
3. Trasy prowadzenia okablowania z uwzględnieniem dodatkowych przepustów i przekuć i stref pożarowych (uszczelnienie przekuć i przepustów między strefami ppoż). Na potrzeby instalacji można wykorzystać istniejące magistrale okablowania strukturalnego, rozbudowując je w razie potrzeby.
4. Liczbę i lokalizację w poszczególnych węzłach przełączników sieciowych niezbędnych do instalowanych komunikacji urządzeń systemu.
5. Uzgodnienia i dostosowanie instalacji do przepisów ppoż.
6. Plany i schematy z naniesionymi elementami instalacji (czytniki, przyciski, zaczepy, trasy okablowania) na dostarczonych przez inwestora planach w formacie DWG.
7. Uzgodnienie prowadzenia tras wg wytycznych inwestora.

Projekt powinien zostać zaakceptowany przez Inwestora, rzeczoznawcę PPOŻ. W przypadku budynków A i B przed przystąpieniem do realizacji projektu należy uzyskać odpowiednie opinie/zgody konserwatora zabytków. Budynki C, D, E, znajdują się w strefie ochrony konserwatorskiej.

## **Wymagania i funkcjonalności systemu**

W ramach zamówienia Zamawiający dostarczy niezbędne , dożywotnie licencje dla oprogramowania systemu Kontroli Dostępu umożliwiające ewentualną rozbudowę i funkcjonowanie systemu do/dla:

1. 2500przejść (w tym niezbędnych do ich obsługi urządzeń takich jak kontrolery, moduły itp.),
2. 30 000 użytkowników/kart, przy czym zmiana parametrów jednego użytkownika/karty (np. zastąpienie jednej osoby inną dla tej samej karty), nie jest uważane za zwiększenie liczby użytkowników. Ponadto system musi umożliwiać usuwanie nieaktywnych (zgubionych lub uszkodzonych) kart, przy czym istnieje możliwość zwolnienia nie używanego rekordu

oraz jednoczesne użytkowanie (konfigurację systemu, nadawanie uprawnień dla użytkowników i raportowanie zdarzeń itp.) przez co najmniej:

1. 2 administratorów (pełne zarządzanie, kontrola, raportowanie i konfiguracja systemu),
2. 5 Operatorów (nadawanie uprawnień użytkownikom, raportowanie),
3. 9 Portierów (podgląd wybranych zdarzeń i alarmów).

### **3.1. Specyfikacja funkcjonalności Systemu KD wymaganych bezwzględnie na dzień złożenia oferty.**

### **3.1.1 Struktura systemu, zarządzanie i konfiguracja.**

Wymagane cechy techniczne, jakościowe i funkcjonalne:

|  |  |
| --- | --- |
| 1 | Infrastruktura systemu oparta o technologię IP. Komunikacja pomiędzy urządzeniami systemu tj. serwery, stanowiska administratorów i operatorów, kontrolery musi odbywać się za pośrednictwem sieci LAN i standardowego protokołu TCP/IP (IPv4 i IPv6). |
| 2 | Scentralizowana obsługa systemu umożliwiająca zarządzanie całą infrastrukturą, poświadczeniami i użytkownikami z jednego miejsca (oprogramowania). |
| 3 | Obsługa przez system wielu rodzajów urządzeń sprzętowych powiązanych w grupy np. kontrolery z jednym czytnikiem, kontrolery z 2 czytnikami, zintegrowane czytniki i kontrolery drzwi oraz kontrolery drzwi z włączoną funkcją Power-over-Ethernet (PoE). |
| 4 | Obsługa protokołu OSDP z szyfrowaniem min AES 128 bit na magistrali szeregowej RS485 |
| 5 | Odczytywanie obiektu SIO wgranego na kartę typu MIFARE (13,56MHz). |
| 6 | Globalna funkcja „antipasspback” w trybie online oraz w trybie offline w przypadku utraty komunikacji z serwerem. |
| 7 | Możliwość tworzenia i obsługi zdefiniowanych scenariuszy bezpieczeństwa. |
| 8 | Konfiguracja uprawnień dla obsługi i administracji (np. w ramach poszczególnych budynków lub grupy użytkowników lub poświadczeń) |
| 9 | Obsługa funkcjonalności programu przy pomocy utworzonych pulpitów nawigacyjnych. Konfiguracja powinna umożliwiać tworzenie w okienku pulpitu nawigacyjnego widżetów z możliwością określenia ich lokalizacji i rozmiaru, tytułu widżetu, koloru tła widżetu oraz możliwości okresowego odświeżania zawartości widżetu. Typami widżetów pulpitu nawigacyjnego będą: obraz - umożliwia wyświetlanie obrazu (JPG, PNG, GIF, BMP) na pulpicie nawigacyjnym. tekst - umożliwia wyświetlanie tekstu na pulpicie nawigacyjnym. Styl tekstu musi być konfigurowalny, aby użytkownik mógł określić czcionkę, rozmiar, kolor i wyrównanie tekstu.  kafelek - umożliwia wyświetlanie dowolnego obiektu z USP wewnątrz kafelka.  strona internetowa: umożliwia wyświetlanie adresu URL na pulpicie nawigacyjnym. |
| 10 | Oprogramowanie musi umożliwiać indywidualne ustawianie interfejsów (pulpitów nawigacyjnych) dla administratora lub użytkownika (lub grup użytkowników), w zależności od nadanych uprawnień. Wybrani użytkownicy lub grupy nie powinny mieć możliwości zmiany tych ustawień. |
| 11 | Nadawanie uprawnień poszczególnym użytkownikom systemu zarządzania w zależności od stanowiska (administrator, operator, portier itp.) z możliwością ograniczania uprawnień w zadanych przedziałach czasowych oraz zmiany tych uprawnień dla całej grupy. |
| 12 | Struktura oprogramowania musi umożliwiać dopasowanie funkcjonalności udostępnianych przez program odpowiednio do potrzeb danego stanowiska pracy (administrator, operator, portier itp.) – w zależności od użytkowanego na danym stanowisku modułu aplikacji lub/i uprawnień użytkownika. |
| 13 | Możliwość tworzenia polityk haseł dla użytkowników. |
| 14 | Pulpity nawigacyjne będą dzielone w folderze prywatnym lub publicznym. |
| 15 | Możliwość obsługi w przyszłości systemu rozbudowanego o kolejne przejścia minimum do 2500 przejść. |
| 16 | Definiowanie kalendarza świąt uwzględniającego opcję automatycznego nadawania/blokowania dostępu do wskazanych przejść lub grup przejść oraz dla wskazanych poświadczeń lub grup poświadczeń. |
| 17 | Oprogramowanie klienta musi zapewniać dostęp lokalny (na serwerze i stacjach operatorskich z zainstalowanym dedykowanym oprogramowaniem typu klient) oraz za pomocą zdalnego połączenia z opcją przejęcia lub podglądu stacji operatorskiej. |
| 18 | Aplikacja obsługująca system musi obsługiwać 64-bitowy tryb pracy. |
| 19 | Wszystkie aplikacje obsługujące system powinny zapewniać mechanizm uwierzytelniania i autoryzacji użytkowników. W związku z tym administrator (z odpowiednimi uprawnieniami) może zdefiniować określone prawa dostępu i uprawnienia dla każdego użytkownika w systemie. |
| 20 | Pełna obsługa aplikacji w języku polskim i angielskim. |
| 21 | Oprogramowanie zainstalowane na serwerze musi utrzymywać łącze komunikacyjne z kontrolerami sprzętowymi, w sposób ciągły monitorować, czy kontrolery są w trybie online, czy offline oraz sygnalizować stan pracy systemu, w tym na przykład brak połączenia z elementami systemu lub awarie . |
| 22 | Zarządzanie uprawnieniami użytkownika(karty) typu gość - np. określenie terminu ważności (od do) |
| 23 | Opcja aktywacji lub wyłączenia profilu posiadacza karty: aktywacja profilu posiadacza karty od zadanego czasu i daty, wygaśnięcie uprawnień w oparciu o datę pierwszego użycia poświadczeń lub wygaśnięcie w dniu zdefiniowanym przez uprawnionego użytkownika. |
| 24 | Grupowa aktywacja, dezaktywacja lub reaktywacja użytkowników. |
| 25 | Możliwość przypisania kilku kart lub poświadczeń dla pojedynczego użytkownika. |
| 26 | Konfiguracja grup uprawnień do przejść z jednoczesną możliwością nadawania dodatkowych, indywidualnych, uprawnień poza grupami. |
| 27 | Obsługa zaawansowanego zarządzania przejściami w zakresie: a) Jednoczesnego odblokowania wszystkich drzwi z danego obszaru. b) Konfigurowania trybu ponownego blokowania przejścia w momencie otwarcia drzwi, po określonym czasie lub w momencie zamknięcia drzwi. c) Określenia zasad dostępu dla innych posiadaczy kart, gdy osoba nadzorująca wejdzie na dany obszar. d) włączenia harmonogramu odblokowywania drzwi po wejściu pracownika do obiektu. e) uruchomienia harmonogramów i wyjątków od uruchomienia harmonogramów przyporządkowanych do przejść. Uruchomiony harmonogram ma określać kiedy drzwi powinny zostać automatycznie odblokowane lub zablokowane. Obsługa określonego harmonogramu odblokowania offline. Wyjątki od harmonogramów - określenie okresów, w których harmonogramy nie będą stosowane, na przykład w dni ustawowo wolne od pracy. f) Możliwości przypisania przynajmniej jednej kamery do przejścia. Materiał wizyjny musi być powiązany ze zdarzeniami dostępu do drzwi, takimi jak przyznanie lub odmowa dostępu. |
| 28 | Zliczanie osób i śledzenie obecności w obszarze z automatycznym alarmem w przypadku przekroczenia zdefiniowanego maksymalnego dopuszczalnej, maksymalnej liczby. |
| 29 | Obsługa niestandardowych pól w bazie systemu (pola definiowane przez użytkownika) a) Tworzenie i obsługa kilku pól niestandardowych. b) Stosowanie w/w pól dla posiadaczy kart, grup, poświadczeń i gości. c) Rodzaje obsługiwanych pól niestandardowych: tekst, liczby całkowite, liczby dziesiętne, daty, typ logiczny i obrazy (grafika). d) Możliwość definiowania wartości domyślnych. e) Wykorzystanie pól niestandardowych do zapytań i generowania raportów. |
| 30 | Możliwość zarządzenia użytkownikami podglądu zdarzeń systemu kontroli dostępu za pomocą przeglądarki www. |
| 31 | Oprogramowanie powinno być dostosowane do pracy w środowisku Windows Serwer Datacenter 2016 lub 2019 na maszynie wirtualnej udostępnionej przez Zamawiającego. |
| 32 | Możliwość logowania do aplikacji przy użyciu lokalnie przechowywanych kont użytkowników i haseł lub przy użyciu poświadczeń usługi Active Directory. |
| 33 | Oprogramowanie musi być oparte na otwartej architekturze umożliwiającej konfigurację i zarządzanie urządzeniami systemu kontroli dostępu pochodzącymi od różnych producentów. System powinien mieć możliwość integracji z różnymi modułami (w tym istniejący ALPR Genetec), kontrolerami, czytnikami kart i aplikacjami wchodzącymi w skład systemów innych niż oferowany (w przyszłości istniejący system KD BOSCH) w zakresie obsługi baz użytkowników i uprawnień oraz monitorowania pracy tych systemów. |
| 34 | Oprogramowanie zainstalowane na serwerze musi przeprowadzać synchronizację wszystkich kontrolowanych przez to oprogramowanie urządzeń kontroli dostępu, takich jak np. kontrolery obsługujące poszczególne przejścia lub moduły we/wy oraz weryfikować i rejestrować wszystkie działania i zdarzenia związane z dostępem, gdy kontrolery drzwi i moduły we/wy są w trybie online. |
| 35 | Synchronizacja jednostek sprzętowych musi być zautomatyzowana i przejrzysta dla użytkowników z możliwością ręcznej synchronizacji jednostek lub synchronizacji jednostek według harmonogramu |
| 36 | Interfejs monitorowania pracy systemu musi obsługiwać zarówno raportowanie za pomocą jednego kliknięcia w przypadku systemu kontroli dostępu i integrowanego systemu ALPR a w przyszłości systemu nadzoru wizyjnego, jak również śledzenie obszarów, kamer, drzwi, stref, posiadaczy kart, wind, jednostek LPR i innych za pomocą jednego kliknięcia. Raportowanie lub śledzenie za pomocą jednego kliknięcia ma tworzyć nowe zadanie z wybranymi jednostkami do raportowania lub śledzenia. |
| 37 | Wsparcie dla synchronizacji posiadaczy kart i grup posiadaczy kart za pośrednictwem usługi Active Directory, w tym poświadczeń i zdjęć posiadaczy kart. Możliwość importowania posiadaczy kart z usługi Azure AD. |
| 38 | Zapewnienie przepływu zadań dotyczących wydawania identyfikatorów i wniosków o kartę. |
| 39 | Natywne tworzenie poświadczeń mobilnych w oparciu o technologię SIO i zarządzanie nimi w taki sam sposób, jak innymi poświadczeniami. |
| 40 | Możliwość drukowania identyfikatorów i tworzenie szablonów z obsługą drukowania masowego identyfikatorów dwustronnych. |
| 41 | Zliczanie osób, śledzenie obecności w obszarze i obsługa zbiórki w przypadku alarmu pożarowego. |
| 42 | Wsparcie konfiguracji urządzenia za pomocą wstępnie skonfigurowanego szablonu przejść. |
| 43 | Automatyczne wykrywanie dołączanych urządzeń i ich rodzajów z wykorzystaniem dedykowanych portów. |
| 44 | Możliwość wymiany urządzenia (np. istniejącego kontrolera na nowy) z jednoczesnym przechowaniem dzienników i zdarzeń ze starej jednostki. |
| 45 | Możliwość wstępnej konfiguracji systemu przed fizyczną instalacją sprzętu. |
| 46 | Możliwość zbiorczej aktualizacji oprogramowania układowego |
| 47 | Unifikacja zarządzaniem systemami kontroli dostępu, nadzoru wizyjnego i LPR  a) Interfejs monitorowania powinien przedstawiać rzeczywisty zunifikowany interfejs bezpieczeństwa do monitorowania i raportowania ACS, VMS i ALPR. Zaawansowany podgląd na żywo i odtwarzanie zarchiwizowanych materiałów wizyjnych będzie możliwe za pośrednictwem interfejsu monitorowania.  b) Interfejs konfiguracji powinien przedstawiać rzeczywisty zunifikowany interfejs bezpieczeństwa do konfiguracji i zarządzania ACS, VMS i ALPR. c) Użytkownik będzie mógł powiązać jedną lub więcej kamer wideo z następującymi typami jednostek: obszary, drzwi, windy, strefy, alarmy, panele antywłamaniowe, kamery LPR i inne. d) Możliwość implementacji w systemie dedykowanych kamer monitoringu wizyjnego. Korelacji przesyłanego i nagranego za ich pomocą obrazu z wybranymi zaistniałymi w systemie zdarzeniami dla danego przejścia (także ALPR). |
| 48 | System musi docelowo umożliwiać wsparcie i możliwość integracji innych systemów zewnętrznych. Powinien zawierać funkcje i cechy umożliwiające obsługę dodawanych w przyszłości nowych elementów do integracji z systemami zewnętrznymi, takimi jak:  a) zewnętrzne systemy nadzoru wizyjnego, b) zewnętrzne systemy kontroli dostępu (w szczególności istniejący system KD firmy BOSCH), c) integracja LPR z kasami parkingowymi,  d) systemy zarządzania budynkiem, e) środowisko kontroli dostępu (skaner identyfikatorów, synchronizacja kart, Guardtour), f) protokoły danych (modbus, BacNet, OPC, SNMP), g) ściana wizyjna, h) systemy zarządzania zasobami ludzkimi (HRMS). |
| 49 | Dla zapewnienia odpowiedniego poziomu i ciągłości pracy system KD musi umożliwiać:  a) Zapewnienie dynamicznej rezerwy zarządzania systemem – możliwość natychmiastowej gotowości do przejęcia przez serwer zapasowy roli serwera podstawowego. Przełączenie awaryjne musi nastąpić w czasie krótszym niż 1 minuta bez działania użytkownika. b) Redundancję na poziomie katalogów z konfiguracją oraz kontrolerów obsługujących przejścia. c) Synchronizację katalogu rezerwowego bazy danych konfiguracji z katalogiem podstawowym. d) Samokontrolę i automatyczna synchronizację katalogów z opcją odzyskiwania i synchronizacji odzyskanych danych po awarii. Synchronizacja baz danych konfiguracji powinna odbywać się przy użyciu mechanizmu tworzenia kopii zapasowych i przywracania z możliwością ustawienia okresu synchronizacji. |
| 50 | W przypadku rozszerzenia systemu o obsługę dodatkowych modułów wizyjnych system powinien umożliwiać synchronizację baz danych konfiguracji w czasie rzeczywistym za pomocą funkcji SQL Mirroring lub SQL Always On. |
| 51 | System musi umożliwiać unieważnienie poświadczeń kontroli dostępu z możliwością zwolnienia nieużywanego rekordu, bez kasowania danych z zachowaniem rekordów historycznych. |
| 52 | W przypadku utraty połączenia z serwerem system musi zapewniać ciągłość pracy kontrolerów, modułów drzwiowych i czytników i zapisywanie zdarzeń, logów z przejść podłączonych do tych jednostek. |
| 53 | System ma zapewniać zapisywanie konfiguracji dla kontrolera, grup kontrolerów, grup modułów drzwiowych i łatwe zaimplementowanie konfiguracji w przypadku awarii kontrolera, a także przeniesienie ustawień konfiguracji grup przejść zależnych od danego kontrolera do innego kontrolera w celu zachowania ciągłości pracy. |

### **3.1.2 Monitorowanie pracy systemu, alarmy i raportowanie.**

Wymagane cechy techniczne, jakościowe i funkcjonalne:

|  |  |
| --- | --- |
| 1 | Monitorowanie zdarzeń bieżących i ich odtwarzanie w czasie rzeczywistym. |
| 2 | Zarządzanie alarmami w czasie rzeczywistym. |
| 3 | Raportowanie oraz tworzenie niestandardowych szablonów raportów w oparciu o skonfigurowane pulpity zadań. |
| 4 | Interfejs systemu ma umożliwiać dostęp do monitorowania jego pracy obejmującego między innymi: alarmy i inne zdarzenia, monitorowanie komunikacji z poszczególnymi elementami systemu. |
| 5 | Możliwość wyświetlania zapisanych w systemie raportów. Wyświetlane dane następuje przez pokazanie całkowitej liczby wyników w raporcie, zestawu najlepszych wyników z raportu, albo wizualnego wykresu z danymi zawartymi w raporcie. |
| 6 | Funkcja automatycznego wysyłania powiadomienia (mail) w przypadku alarmu związanego z nieuprawnionym lub niezgodnym z harmonogramem użyciem wskazanego przejścia. Jeżeli przejście monitorowane będzie dodaną do systemu, dedykowaną kamerą - załączenie zdjęcia z tej kamery. |
| 7 | Raportowanie stanu aktualizacji oprogramowania urządzeń takich jak np. kontrolery oraz moduły drzwiowe |
| 8 | Obsługa nieograniczonej liczby dzienników i zdarzeń historycznych (w tym alarmy). Jedyne dozwolone ograniczenie, to ilość dostępnego miejsca na dysku twardym. |
| 9 | Funkcja monitorowania stanu przejścia (przewodowe). |
| 10 | Monitorowanie autoryzacji użytkownika/karty na przejściach bezprzewodowych |
| 11 | Funkcja monitorowania stanu baterii w przypadku zastosowania okuć bezprzewodowych. |
| 12 | Funkcja raportowania o zdarzeniach z wykorzystaniem rozbudowanych filtrów umożliwiająca prezentację danych dotyczących przejścia, karty(użytkownika), grupy przejść lub kart użytkowników w zależności od daty itp. Możliwość natychmiastowego możliwość eksportu lub druku do plików typu pdf, html, docx, xlsx, csv. |
| 13 | Automatyczne raportowanie o zdarzeniach z wykorzystaniem rozbudowanych filtrów umożliwiająca prezentację danych dotyczących przejścia, karty(użytkownika), grupy przejść lub kart użytkowników w zależności od daty itp. Możliwość natychmiastowego możliwość eksportu lub druku do plików typu pdf, html, docx, xlsx, csv. |
| 14 | Automatyczne raportowanie o zdarzeniach dla danego, wskazanego pracownika oraz gościa (raportowanie za zadany okres). |
| 15 | Dostęp do logów operacji – monitorowanie / śledzenie operacji użytkowników. |
| 16 | Monitorowanie stanu technicznego. a) Monitorowanie stanu technicznego systemu, rejestracja zdarzeń związanych ze stanem i obliczanie statystyk dla poszczególnych zdarzeń. b) Obliczanie statystyk w określonym przedziale czasowym (godziny, dni, miesiące). c) Dostęp do danych związanych z monitorowaniem z poziomu raportów bieżących i historycznych. |
| 17 | Zarządzanie alarmami w oprogramowaniu. a) Tworzenie i modyfikowanie alarmów zdefiniowanych przez użytkownika. Obsługa nieograniczonej liczby alarmów zdefiniowanych przez użytkownika. b) Przypisanie harmonogramu lub okresu obowiązywania do alarmu. Alarm zostanie wyzwolony tylko wtedy, gdy jest aktualny dla bieżącego okresu. c) Ustawienie priorytetu alarmu i warunku ponownego włączenia. d) Ustawienie opcji wyświetlania bieżącego lub nagranego materiału wizyjnego, stopklatki lub ich połączenie po wyzwoleniu alarmu. e) Możliwość grupowania alarmów według źródła i typu. f) Określenie czasu, po którym alarm będzie automatycznie potwierdzany. g) Określenie odbiorców alarmu. Powiadomienia alarmowe są kierowane do jednego lub większej liczby odbiorców. Odbiorcom należy przypisać priorytet, który ustala kolejność odbioru alarmu. h) Zdefiniowanie trybu emisji alarmu. Powiadomienia o alarmach należy wysyłać w trybie transmisji sekwencyjnej lub jednorazowej. i) Określenie, czy wyświetlać źródło alarmu, jeden lub więcej elementów, czy stronę HTML. j) konfiguracja opcji obowiązkowego wysłania raportu dotyczącego zdarzenia podczas jego potwierdzania. k) Interfejs powinien obsługiwać powiadomienia alarmowe wysyłane na adres e-mail lub dowolne urządzenie korzystające z protokołu SMTP. l) Użytkownik powinien mieć możliwość potwierdzania alarmów, wysłania z systemu raportu o zaistniałym zdarzeniu po potwierdzeniu alarmu oraz przełączania alarmu w tryb cichy. m) Alarm powinien być skonfigurowany w taki sposób, aby pozostawał widoczny do momentu potwierdzenia. |
| 18 | Możliwość weryfikacji przyczyny alarmu bez jego potwierdzenia. |

### **3.1.3 Kontrolery i moduły rozszerzające.**

Ze względu na konieczność obsługiwania dużej liczby poszczególnych elementów systemu, kontrolery muszą charakteryzować się natywną komunikacją oraz wysoką wydajnością, co umożliwi ich działanie niezależnie od liczby połączonych hostów aplikacji do kontroli dostępu.

Wymagane cechy techniczne, jakościowe i funkcjonalne kontrolerów:

|  |  |
| --- | --- |
| 1 | Możliwość obsługi min. 64 przejść przez jeden kontroler, z wykorzystaniem modułów rozszerzających. |
| 2 | Obsługa protokołów OSDP, bezpiecznego OSDP, Wiegand. |
| 3 | Obsługa czytników biometrycznych, pasków magnetycznych, czytników F/2F i jego nadzorowanych technologii. |
| 4 | Obsługa klawiatury oraz możliwość odczytywania zawartych w przesyłanych w komunikacji szeregowej danych informacji o dacie i godzinie. |
| 5 | Wbudowany układ pamięci kryptograficznej i szyfrowanie danych. |
| 6 | Komunikacja hosta chroniona przez TLS 1.2/1.1 |
| 7 | Złącze rozszerzające kontroler/IO chronione przez AES (seria 3 SIO) |
| 8 | Kontrola dostępu do sieci za pomocą 802.1X |
| 9 | Wsparcie dla OpenSSL |
| 10 | Możliwość zachowania danych przez okres min. 3 miesiący po utracie zasilania |
| 11 | Możliwość podłączenia min 4 czytników z użyciem protokołu OSDP. |
| 12 | Min. 6 wejść monitorujących oraz min 4 wyjścia przekaźnikowe. |
| 13 | Moduł wspiera łączenie aktywności innych urządzeń w obrębie systemu w celu generowania działań zaprogramowanych przez system. |
| 14 | Globalna funkcja „antipasspback” w trybie online oraz w trybie offline |

Wymagane cechy techniczne, jakościowe i funkcjonalne modułów rozszerzających:

|  |  |
| --- | --- |
| 1 | Obsługa protokołów OSDP v1 i v2. |
| 2 | Możliwość podłączenia min 2 czytników za pomocą protokołu OSDP. |
| 3 | Minimum 8 wejść programowalnych, minimum 1 wejście typu tamper, minimum 1 wejście awarii zasilania oraz min. 6 wyjść przekaźnikowych i obsługa min. 1 magistrali RS 485 |
| 4 | Wbudowany układ pamięci kryptograficznej i szyfrowanie danych, komunikacja zabezpieczona przez TLS 1.2/1.1 lub AES-256/128 |

### **3.1.4 Czytniki kart.**

Czytniki zbliżeniowe zainstalowane do odczytu kart, muszą obsługiwać protokół OSDP. Rozmiar czytników nie powinien przekraczać 5x12x3 cm i powinny one być przeznaczone do montażu na ościeżnicach drzwiowych, ścianach lub dowolnych innych płaskich powierzchniach – wewnątrz i na zewnątrz budynku.

Wymagane cechy techniczne, jakościowe i funkcjonalne:

|  |  |
| --- | --- |
| 1 | Obsługa protokołu OSDP |
| 2 | Współpraca z kartami 13,56 MHz: - MIFARE Classic i MIFARE DESFire EV1; - iCLASS SE; - ISO14443A (MIFARE) CSN, ISO14443B CSN, ISO15693 CSN; - FeliCa™4 CSN, CEPAS4 CSN or CAN. |
| 3 | Czytniki kart zbliżeniowych jest kompatybilny z modelem danych Secure Identity Object™ (SIO) i wspiera poświadczenia Secure Identity Object™ (SIO) |
| 4 | Poświadczenia SIO mogą znajdować się na dowolnej liczbie nośników, takich jak karty zbliżeniowe iCLASS Seos, iCLASS SE, MIFARE Classic oraz MIFARE DESFire EV1. |
| 5 | Zaawansowane funkcje związane z pracą oraz wydajnością czytnika: a) zmiana priorytetów odczytu dla dualnych kart zbliżeniowych z podwójnym układem wysokich częstotliwości (13.56 MHz). Zmiana priorytetu jednej technologii pomaga w jej odczycie jako pierwszej w momencie zbliżenia karty do czytnika, ograniczając w ten sposób ilość odczytów drugiej technologii. b) możliwość zmiany konfiguracji związanej z obsługą konkretnych typów kart, w celu możliwości podniesienia poziomu bezpieczeństwa w przyszłości lub w przypadku migracji ze starszego standardu na nowy. c) możliwość zmiany konfiguracji jego aplikacji z wykorzystaniem konfiguracyjnych kart firmware’owych. Funkcja umożliwia zmianę funkcjonalności poprzednio zainstalowanych czytników i dostosowaniu ich do zmian w późniejszym czasie. |
| 6 | Czytnik powinien umożliwiać konfigurację funkcji Velocity Checking (kontrola prędkości danych) w celu zabezpieczenia przed atakami elektronicznymi, opartymi na wielokrotnych próbach uwierzytelnienia |
| 7 | Odczytywanie obiektu SIO wgranego na kartę typu MIFARE (13,56MHz) przez czytniki. |
| 8 | Zakres temperatur pracy: nie węższy niż od -30℃ do 60℃ |
| 9 | Klasa środowiskowa IP65 |

Dodatkowo czytniki powinny realizować zaawansowane funkcje związane z jego pracą oraz wydajnością, a w szczególności:

1. umożliwiać zmianę priorytetów odczytu dla dualnych kart zbliżeniowych z podwójnym układem wysokich częstotliwości (13.56 MHz). Zmiana priorytetu jednej technologii pomaga w jej odczycie jako pierwszej w momencie zbliżenia karty do czytnika, ograniczając w ten sposób ilość odczytów drugiej technologii.
2. umożliwiać zmianę konfiguracji związanej z obsługą konkretnych typów kart, w celu możliwości podniesienia poziomu bezpieczeństwa w przyszłości lub w przypadku migracji ze starszego standardu na nowy.
3. pozwalać na zmianę konfiguracji jego aplikacji z wykorzystaniem konfiguracyjnych kart firmware’owych. Funkcja umożliwia zmianę funkcjonalności poprzednio zainstalowanych czytników i dostosowaniu ich do zmian w późniejszym czasie.

Dla zapewnienia możliwości rozszerzenia funkcjonalności w przyszłości zaprojektowane czytniki umożliwiają doposażenie ich o moduł bluetooth bez konieczności wymiany zainstalowanego już urządzenia.

W systemie będą stosowane kompatybilne karty zbliżeniowe SEOS. Wymiary kart użytych w projekcie mają być zgodne ze standardem wymiarów karty płatniczej.

## **Przejścia**

Wszystkie przejścia jednostronne muszą zostać zamontowane w taki sposób, aby wejście do pomieszczenia było możliwe dzięki użyciu karty z odpowiednimi uprawnieniami lub klucza dopasowanego do istniejącej wkładki, natomiast wyjście umożliwiać będzie klamka lub przycisk zwalniający blokadę. Użycie przycisku powinno być rejestrowane przez oprogramowanie systemu i dostępne w historii zdarzeń dla danego przejścia.

Przejścia dwustronne powinny być wyposażone w czytniki kart po obu stronach oraz odpowiednie zabezpieczenia zwalniające blokady w przypadku pożaru. W tego typu przejściach należy zdemontować istniejące klamki i zamontować gałki uniemożliwiające otworzenie drzwi bez autoryzacji lub klucza.

W obu typach przejść należy zainstalować kontaktrony przekazujące do systemu informacje o otwarciu drzwi.

Dla przejść wymienionych w załączniku nr 7 do SIWZ przewiduje się montaż trzech typów blokad.

### **4.1. Elektrozaczep**

Dla przejść ewakuacyjnych, (również ppoż) wymagany montaż elektrozaczepu rewersyjnego (NO), zapewniający otwarcie drzwi przy naporze do 3000N. Inne wymagania to :możliwość montażu do drzwi lewych i prawych oraz montażu w poziomie.

1. siła trzymania 3000N, testowany na 500 000 tysięcy cykli.
2. głębokość zachodzenia zapadki 6mm.
3. zwiększona ochrona przed manipulacją elektrozaczepem poprzez ograniczenie dostępu do zapadki. styki monitoringu zintegrowane w obudowie.
4. wyposażony w potencjałowe wyjście informujące o położeniu zapadki wewnętrznej.
5. zakres temperatury pracy: -15 °C +40 °C. Certyfikowany na zgodność z normą EN 13637.

Minimalne wymagania dla elektrozaczepów montowanych w pozostałych przejściach:

1. elektrozaczep rewersyjny (NO) z czujnikiem i monitoringiem,
2. zapadka regulowana: 3 mm,
3. dzięki symetrycznej obudowie może być stosowany do drzwi lewych i prawych oraz może być montowany w poziomie,
4. wytrzymałość mechaniczna 3500 N. Zakres temperatury pracy -15 °C +40 °C,
5. maksymalny nacisk na zapadkę 10 N (ok. 1 kg).

### **4.2. Zwora elektromagnetyczna**

Montowane elementy tego typu powinny spełniać poniższe wymagania:

1. montaż nawierzchniowy,
2. siła przyciągania dla drzwi jednostronnych ma być nie mniejsza niż 270 kg, a dla drzwi dwuskrzydłowych 540 kg,
3. możliwość zasilania prądem o napięciu 12 lub 24V.
4. element musi być wyposażona w kontaktron I czujnik Halla.

### **4.3. Okucia bezprzewodowe.**

Dla wyznaczonych przejść przewiduje się instalację elektronicznych okuć zintegrowanych z funkcjonalnością kontroli dostępu. Urządzenia muszą obsługiwać ten sam standard kart i poświadczeń, jak w wypadku opisanych wyżej czytników i przewodowych podłączanych do modułów interfejsów. W przypadku domów studenckich należy w okuciach zamontować istniejące wkładki ze względu na stosowany system jednego klucza typu master do otwierania wszystkich zamków.

Wymagane cechy techniczne i funkcjonalne okuć:

1. Zintegrowany multi-technologiczny czytnik zbliżeniowy z możliwością odczytu:
2. numerów seryjnych procesorów kart Mifare Classic/Mifare Plus/Mifare DESFire CSN (ISO 14443A) lub danych z sektorów pamięci;
3. numerów seryjnych kart iCLASS/iCLASS SE CSN (ISO 15693)/iCLASS Seos lub danych z sektorów pamięci;
4. szyfrowanych danych w standardzie SIO (Secure Identity Object);
5. Dostępny tryb pracy typu office (dwukrotne przyłożenie transpondera otwiera drzwi na stałe i ponowne dwukrotne przyłożenie zamyka na stałe).
6. Dane dotyczące użytkowników oraz ich kart dostępowych/kodów PIN muszą być przechowywane zarówno w aplikacji odpowiedzialnej za kontrolę dostępu, jak i w sterownikach drzwiowych (dostępy poszczególnych drzwi/grup, godziny, harmonogramy czasowe, kalendarz).
7. Komunikacja z systemem kontroli dostępu powinna być realizowana z wykorzystaniem protokołu TCP/IP, a autoryzacja przeprowadzana przez system KD
8. Luźna klamka zewnętrzna - klamka wewnętrzna zasprzęglona na stałe (swobodne wyjście)
9. Możliwość przechowywania w pamięci minimum 10 awaryjnych kart (używanych wyłącznie w przypadku utraty komunikacji z anteną radiową/kontrolerem drzwiowym)
10. Diody LED do wizualizacji stanu pracy.
11. Odległość odczytu do 40mm.
12. Zgodność z IP 52 (drzwi wewnętrzne) oraz IP54 (drzwi zewnętrzne)
13. Wymiary nie przekraczające 315 x 45 x 10/20 mm (H x W x D)
14. Standard radiowy IEEE 802.15.4 (2.4 GHz)
15. Zakres temperatur pracy od 0°C do 60°C
16. Dopuszczalna grubość drzwi od 40 do 100 mm
17. Zasilanie bateryjne – żywotność nie mniej jak 30 000 cykli
18. Monitorowanie stanu drzwi, użycia klamki lub otworzenia drzwi z użyciem klucza.

W przypadku zastosowania dedykowanych do komunikacji modułów wymagane są następujące cechy techniczne i funkcjonalne:

1. Połączenie z systemem kontroli dostępu za pomocą magistrali TCP/IP (adresowalnej).
2. Możliwość podłączenia minimum 16 urządzeń radiowych (okuć lub zamków bezprzewodowych) za pomocą jednej anteny.
3. Zintegrowany bufor pamięci dla rejestracji zdarzeń i uprawnień identyfikatorów.
4. Możliwość pracy w trybie on-line i offline.
5. Zintegrowana antena z możliwością montażu anteny zewnętrznej .
6. Zaszyfrowana komunikacja radiowa (AES 128 bit).
7. Diody LED do wizualizacji stanu pracy.
8. Aprobaty CE, ETL, FCC, IC, C-Tick.
9. Zasilanie PoE.
10. Standard radiowy IEEE 802.15.4 (2.4 GHz) - 16 kanałów (11-26).
11. Możliwość osiągnięcia zasięgu powyżej 30m.
12. Czułość odbiornika nie mniej niż 100dBm.
13. Bezprzewodowa moc transmisji nie mniej niż 10 dBm/MHz.

Instalowany system powinien umożliwiać Integrację systemu przewodowego i okuć bezprzewodowych. Konfiguracja, monitorowanie i zarządzanie systemem powinno odbywać się w jednym programie.

## **Dokumentacja powykonawcza**

Po zakończeniu prac instalacyjnych i konfiguracyjnych systemu Wykonawca przekaże Inwestorowi dokumentację powykonawczą zawierającą:

1. Plany poszczególnych budynków z naniesionymi elementami instalacji (czytniki, przyciski, zaczepy, trasy okablowania).
2. Zestawienie zawierające lokalizację poszczególnych kontrolerów z listą podpiętych do nich przejść.
3. Schemat instalacji i podłączenia elementów systemu.

Dokumentacja zostanie dostarczona w formie papierowej w liczbie egzemplarzy 1 szt. oraz w wersji elektronicznej w formacie dwg lub innym wraz z przeglądarką umożliwiającą odczyt i przeglądanie dokumentacji.

## **Usługa serwisu**

Przez okres 24 miesięcy od daty odbioru końcowego Wykonawca będzie świadczył Zamawiającemu usługę serwisu polegającą na pomocy w sprawnym zarządzaniu systemem kontroli dostępu oraz jego konfigurowaniu, a także usuwaniu problemów z bieżącym funkcjonowaniem tego systemu nie mających charakteru wady lub nie podlegających naprawie z tytułu gwarancji lub rękojmi w liczbie 20 godzin dla każdego oddanego budynku.

W przypadku wystąpienia problemu krytycznego uniemożliwiającego pracę całego systemu Uczelni lub systemu w całym budynku czas reakcji wynosi 4 godziny od momentu zgłoszenia problemu. Przez czas reakcji na zgłoszenie problemu krytycznego Zamawiający rozumie czas, jaki upłynie od zgłoszenia awarii do nawiązania kontaktu przez pracownika Wykonawcy ze zgłaszającym awarię pracownikiem Zamawiającego w celu przeprowadzenia wstępnej diagnostyki i w miarę możliwości przekazania zaleceń.

W przypadku wystąpienia problemu niekrytycznego uniemożliwiającego pracę jednego lub kilku przejść lub problemów dla pojedynczych kart dostępu lub problemów z konfiguracją systemu, z którymi czas reakcji wynosi 24 godziny od momentu zgłoszenia problemu. Przez czas reakcji na zgłoszenie problemu krytycznego Zamawiający rozumie czas, jaki upłynie od zgłoszenia problemu do nawiązania kontaktu przez pracownika Wykonawcy ze zgłaszającym problem pracownikiem Zamawiającego w celu przeprowadzenia wstępnej diagnostyki i w miarę możliwości przekazania zaleceń.

Czas pracy Wykonawcy powinien być ewidencjonowany dla każdego zgłoszonego przez Zamawiającego problemu i potwierdzony w formie notatki służbowej.