## Założenia ogólne

Celem instalacji systemu jest umożliwienie kontroli dostępu do pomieszczeń we wszystkich budynkach uczelni w tym budynkach administracyjno-dydaktycznych, domach studenckich, SWFiS, archiwum i magazynie, wyszczególnionych w SIWZ, 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 konieczność podłączenia do systemu czujnika umożliwiającego stałe monitorowanie stanu otwarcia/zamknięcia drzwi (kontaktrony).

Podczas instalacji, stosując się do przepisów ppoż, tam gdzie jest to wymagane, działanie systemu (zwolnienie blokady przejść) należy zintegrować 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. zarówno dla istniejącego systemu (budynek CEUE oraz budynek A i B) opartego o kontrolery firmy Bosch, jak i instalowanego systemu, za pomocą jednego oprogramowania, zainstalowanego na udostępnionej przez Zamawiającego maszynie wirtualnej.

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

### 3.1 Ogólne wymagania dotyczące funkcjonalności systemu.

System musi posiadać zgodność z normą: EN-60839-11-1. W ramach realizacji projektu zakłada się wdrożenie spójnego, scentralizowanego z punktu widzenia zarządzania, systemu bezpieczeństwa. W związku z powyższym system musi zapewniać poniższe funkcjonalności:

* Scentralizowaną obsługę i zarządzanie infrastrukturą, użytkownikami i scenariuszami schematami bezpieczeństwa z jednoczesną możliwością wydzielenia stref do niezależnej obsługi i administracji (np. w ramach poszczególnych budynków).
* Opartą o technologię IP infrastrukturę systemu. Komunikacja pomiędzy urządzeniami systemu tj. serwery, stanowiska administratorów i operatorów, kontrolery, moduły sterujące musi odbywać się za pośrednictwem sieci LAN i standardowego protokołu TCP/IP.
* Możliwość zarządzania i integracji z innymi systemami bezpieczeństwa i nadzoru (np. monitoring wizyjny, system kontroli wjazdów itp.).
  + Oprogramowanie do zarządzania bezpieczeństwem musi wspierać bezproblemowe połączenie systemu kontroli dostępu IP (ACS), systemu zarządzania wizyjnego IP (VMS) i automatycznego rozpoznawania tablic rejestracyjnych IP (ALPR) w ramach jednej platformy. Aplikacje interfejsu użytkownika muszą prezentować zunifikowany interfejs bezpieczeństwa do zarządzania, konfigurowania, monitorowania i raportowania systemów ACS, VMS i ALPR oraz powiązanych urządzeń brzegowych.
  + Aplikacja musi zapewniać (w tym dla istniejącego systemu KD) m.in.:

1. Obsługę i konfigurację systemów takich jak ACS, ALPR i VMS.
2. Monitorowanie zdarzeń bieżących i odtwarzanie zarchiwizowanych materiałów wizyjnych.
3. Zarządzanie alarmami.
4. Raportowanie, w tym tworzenie niestandardowych szablonów raportów i raportów o incydentach.
5. Przeglądanie dynamicznych map graficznych.
   * Obsługę minimum 30 tys. użytkowników i 4000 przejść.
   * Obsługę nieograniczonej liczby dzienników i transakcji historycznych (zdarzenia i alarmy). Jedyne dozwolone ograniczenie, to ilość dostępnego miejsca na dysku twardym.
   * Redundancję w przypadku awarii zapewnioną zarówno na poziomie fizycznego serwera, jak i oprogramowania do zarządzania i nadzorowania.
   * Synchronizację jednostek sprzętowych zautomatyzowaną i przejrzystą dla użytkowników z możliwością ręcznej synchronizacji jednostek lub synchronizacji jednostek według harmonogramu.
   * System musi obsługiwać wiele rodzajów urządzeń sprzętowych powiązanych w grupy: kontrolery z jednym czytnikiem, kontrolery z 2 czytnikami, kontrolery z 1 do 64 czytnikami, zintegrowane czytniki i kontrolery drzwi oraz kontrolery drzwi z włączoną funkcją Power-over-Ethernet (PoE).
   * Funkcja monitorowania stanu drzwi zabezpieczonych zarówno system przewodowym, jak i za pomocą okuć bezprzewodowych.
   * Funkcja monitorowania stanu baterii w przypadku zastosowania okuć bezprzewodowych.
   * Funkcja automatycznego wysyłania maila w przypadku alertu o nieuprawnionym lub niezgodnym z harmonogramem wejściem. W przypadku drzwi objętych systemem CCTV możliwość załączenia zdjęcia z kamery.
   * 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 druku oraz możliwość eksportu do plików typu pdf, html, docx, xlsx, csv.
   * Automatyczne raportowanie o zdarzeniach dla danego, wskazanego pracownika oraz gościa (raportowanie za zadany okres).
   * Definiowanie kalendarza świąt (przy automatycznym nadawaniu/blokowaniu dostępu do przejść.
   * Integracja systemu w zakresie zarządzania uprawnieniami dostępu dla kart/użytkowników (w tym harmonogramy), sterowania przejściami i raportowania (użytkownicy, przejścia, kontrolery i zasilanie) z działającym w budynku CEUE systemem KD Bosch oraz systemem kontroli wjazdów i wyjazdów pojazdów opartym o ACS i ALPR (system oparty o oprogramowanie Genetec).
   * Spójne zarządzanie wszystkimi urządzeniami (przewodowymi i bezprzewodowymi) oraz użytkownikami przez jeden interfejs.
   * Dostęp do logów operacji – monitorowanie / śledzenie operacji użytkowników.
   * Bezterminowe licencje na wszystkie aplikacje i moduły oprogramowania wchodzące w skład systemu.

### 3.2 Wymogi oprogramowania:

Oprogramowanie powinno być dostosowane do pracy w środowisku Windows Serwer Datacenter 2016 lub 2019 na maszynie wirtualnej udostępnionej przez Zamawiającego.

Podstawowe cechy i funkcjonalności aplikacji:

* + Oprogramowanie klienta musi zapewniać dostęp lokalny oraz za pomocą zdalnego połączenia.
  + Aplikacja musi obsługiwać 64-bitowy tryb pracy.
  + Wszystkie aplikacje 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.
  + Możliwość logowania do aplikacji przy użyciu lokalnie przechowywanych kont użytkowników i haseł lub przy użyciu poświadczeń usługi Active Directory .
  + Pełna obsługa aplikacji w języku polskim i angielskim.
* Oprogramowanie musi być oparte na otwartej architekturze umożliwiającej konfigurację i zarządzanie urządzeniami systemu kontroli dostępu pochodzącymi od różnych producentów (w tym firmy Bosch oraz Genetec). System powinien mieć możliwość integracji z różnymi modułami, kontrolerami, czytnikami kart i aplikacjami wchodzącymi w skład systemów innych niż oferowany.
* 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.
* 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 .
* Synchronizacja jednostek sprzętowych musi być zautomatyzowana i przejrzysta dla użytkowników z możliwością ręcznej synchronizacji jednostek lub synchronizacji jednostek według harmonogramu.
  + Interfejs monitorowania pracy systemu musi obsługiwać zarówno raportowanie za pomocą jednego kliknięcia w przypadku systemu kontroli dostępu i integrowanych w przyszłości systemów: ALPR i systemu nadzoru wizyjnego, jak również śledzenie obszarów, kamer, drzwi, stref, posiadaczy kart, wind, jednostek ALPR i innych za pomocą jednego kliknięcia. Raportowanie lub śledzenie za pomocą jednego kliknięcia ma tworzyć nowe zadanie z wybranymi jednostkami do raportowania lub śledzenia.
  + Możliwość indywidualnych ustawień interfejsów dla administratora, użytkownika i monitorowania. W zależności od poziomu uprawnień wybrani użytkownicy lub grupy nie powinny mieć możliwości zmiany tych ustawień.
  + Nadawanie uprawnień poszczególnym użytkownikom systemu zarządzania w zależności od stanowiska (administrator, operator, kadry, portier itp.) z możliwością ograniczania uprawnień w zadanych przedziałach czasowych oraz możliwość zmiany tych uprawnień dla całej grupy.
  + Struktura oprogramowania musi umożliwiać dopasowanie funkcjonalności udostępnianych przez program odpowiednio do potrzeb danego stanowiska pracy (administrator, operator, kadry, portier itp.) – w zależności od użytkowanego na danym stanowisku modułu aplikacji lub/i uprawnień użytkownika.
  + 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.
  + Grupowa aktywacja, dezaktywacja lub reaktywacja użytkowników.
  + Możliwość tworzenia polityk haseł dla użytkowników.
  + Możliwość przypisania kilku kart dla pojedynczego użytkownika.
  + Konfiguracja grup uprawnień z jednoczesną możliwością nadawania dodatkowych uprawnień poza grupami.
  + Możliwość wsparcia 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.
  + Zapewnienie przepływu zadań dotyczących wydawania identyfikatorów i wniosków o kartę.
  + Możliwość obsługi natywnie tworzonych identyfikatorów mobilnych i zarządzanie nimi w taki sam sposób, jak innymi poświadczeniami.
  + Możliwość drukowania identyfikatorów i tworzenie szablonów z obsługą drukowania masowego identyfikatorów dwustronnych.
  + Zarządzanie uprawnieniami użytkownika typu gość.
  + Zliczanie osób, śledzenie obecności w obszarze i obsługa zbiórki w przypadku alarmu pożarowego.
  + Możliwość zarządzenia użytkownikami systemu kontroli dostępu za pomocą przeglądarki www.
  + Interfejs systemu umożliwiający dostęp do monitorowania pracy systemu – alerty, zdarzenia, komunikacja z elementami systemu.
  + Usprawnienia w zakresie konfiguracji:

1. Wsparcie konfiguracji urządzenia za pomocą wstępnie skonfigurowanego szablonu przejść.
2. Automatyczne wykrywanie jednostek z wykorzystaniem portów wykrywania i rodzajów wykrywanych jednostek,
3. Możliwość wymiany jednostek (np. istniejącego kontrolera na nowy) z jednoczesnym przechowaniem dzienników i zdarzeń ze starej jednostki.
4. Możliwość wstępnej konfiguracji systemu przed fizyczną instalacją sprzętu.
5. Możliwość zbiorczej aktualizacji oprogramowania układowego z aplikacji.
   * Obsługa zaawansowanego zarządzania przejściami w zakresie:
   1. Jednoczesnego odblokowania wszystkich drzwi z danego obszaru.
   2. Konfigurowania trybu ponownego blokowania przejścia, w momencie otwarcia drzwi, po określonym czasie lub w momencie zamknięcia drzwi.
   3. Określenia zasad dostępu dla innych posiadaczy kart, gdy osoba nadzorująca wejdzie na dany obszar.
   4. Możliwość włączenia harmonogramu odblokowywania drzwi po wejściu pracownika do obiektu.
   5. Odblokowywania harmonogramów i wyjątków od odblokowywanych harmonogramów przyporządkowane do przejść. Harmonogram odblokowywania ma określać, kiedy drzwi powinny zostać automatycznie odblokowane. Obsługa określonego harmonogramu odblokowania offline. Wyjątki od harmonogramów - określenie okresów, w których harmonogramy odblokowania nie będą stosowane, na przykład w dni ustawowo wolne od pracy.
   6. Możliwość korelacji jednej lub więcej kamer do przejścia. Materiał wizyjny ma zostać następnie powiązany ze zdarzeniami dostępu do drzwi, takimi jak przyznanie dostępu lub odmowa dostępu.
   * Zliczanie osób i śledzenie obecności w obszarze z automatycznym alarmem w przypadku przekroczenia zdefiniowanego maksymalnego dopuszczalnego progu.
   * Obsługa pól niestandardowych (pola zdefiniowane przez użytkownika)
6. Tworzenie pól niestandardowych (obsługa min.100 pól).
7. Stosowanie w/w pól dla posiadaczy kart, grup, poświadczeń i gości.
8. Rodzaje obsługiwanych pól niestandardowych: tekst, liczby całkowite, liczby dziesiętne, daty, typ logiczny i obrazy (grafika).
9. Możliwość zdefiniowania wartość domyślnych.
10. Wykorzystanie pól niestandardowych do zapytań i generowania raportów.
11. Możliwość zaimportowania wartości pól niestandardowych za pomocą narzędzia importu.
    * Monitorowanie stanu technicznego.
    1. Monitorowanie stan techniczny systemu, rejestracja zdarzeń związanych ze stanem i obliczanie statystyk dla poszczególnych zdarzeń.
    2. Zapełnienie dziennika zdarzeń Windows zdarzeniami dotyczącymi stanu technicznego związanymi z rolami, usługami i aplikacjami klienta.
    3. Obliczanie statystyk w określonym przedziale czasowym (godziny, dni, miesiące).
    4. Obliczanie dostępności dla klientów, serwerów i jednostek nadzoru wizyjnego / dostępu / ALPR.
    5. Dostęp do danych związanych z monitorowaniem z poziomu raportów bieżących i historycznych.
    * Unifikacja zarządzaniem systemami kontroli dostępu, nadzoru wizyjnego i ALPR
    1. 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.
    2. Interfejs konfiguracji powinien przedstawiać rzeczywisty zunifikowany interfejs bezpieczeństwa do konfiguracji i zarządzania ACS, VMS i ALPR.
    3. Użytkownik będzie mógł powiązać jedną lub więcej kamer wideo z następującymi typami jednostek: obszary, drzwi, windy, strefy, alarmy, panele antywłamaniowe, kamery ALPR i inne.
    4. Podczas przeglądania raportu powinna istnieć możliwość podglądu wideo związanego ze zdarzeniami kontroli dostępu lub incydentami bezpieczeństwa.
    5. Podczas przeglądania raportu powinna istnieć możliwość podglądu materiałów wizyjnych związanych ze zdarzeniami ALPR.

• Zarządzanie alarmami w oprogramowaniu.

* 1. Tworzenie i modyfikowanie alarmów zdefiniowanych przez użytkownika. Obsługa nieograniczonej liczby alarmów zdefiniowanych przez użytkownika.
  2. Przypisanie harmonogramu lub okresu obowiązywania do alarmu. Alarm zostanie wyzwolony tylko wtedy, gdy jest aktualny dla bieżącego okresu.
  3. Ustawienie priorytetu alarmu i progu ponownego włączenia.
  4. Określenie, czy wyświetlać bieżące czy nagrane materiały wizyjne, stopklatki lub ich połączenie po wyzwoleniu alarmu.
  5. Umożliwienie wyświetlania bieżących i nagranych materiałów wizyjnych w tym samym kafelku wideo w trybie obraz w obrazie (PiP).
  6. Możliwość grupowania alarmów według źródła i typu.
  7. Określenie okresu czasu, po którym alarm będzie automatycznie potwierdzany.
  8. Określenie odbiorców alarmu. Powiadomienia alarmowe są kierowane do jednego lub większej liczby odbiorców. Odbiorcom należy przypisać priorytet, który ustala kolejność odbioru alarmu.
  9. Zdefiniowanie trybu emisji alarmu. Powiadomienia o alarmach należy wysyłać w trybie transmisji sekwencyjnej lub jednorazowej.
  10. Określenie, czy wyświetlać źródło alarmu, jeden lub więcej elementów, czy stronę HTML.
  11. Określenie, czy raport zdarzenia jest obowiązkowy podczas potwierdzania.
  12. Przepływy pracy w celu tworzenia, modyfikowania, dodawania instrukcji i procedur oraz potwierdzania alarmu muszą być spójne w przypadku kontroli dostępu, ALPR i alarmów nadzoru wizyjnego.
  13. Interfejs powinien również obsługiwać powiadomienia alarmowe na adres e-mail lub dowolne urządzenie korzystające z protokołu SMTP.
  14. Możliwość tworzenia instrukcji związanych z alarmami powinna być obsługiwana poprzez wyświetlanie jednej lub więcej stron HTML po zdarzeniu alarmowym. Strony HTML powinny być zdefiniowane przez użytkownika i mogą być powiązane.
  15. Obsługiwane jest rozpakowywanie i pakowanie alarmów, gdy wszystkie jednostki powiązane z alarmem mogą być wyświetlane w interfejsie monitorowania za pomocą jednego kliknięcia przycisku.
  16. Użytkownik powinien mieć możliwość potwierdzania alarmów, tworzenia incydentu po potwierdzeniu alarmu i przełączania alarmu w tryb snooze.
  17. Użytkownik powinien móc spontanicznie wyzwalać alarmy w oparciu o coś, co widzi w systemie.
  18. Alarm powinien być skonfigurowany w taki sposób, aby pozostawał widoczny do momentu potwierdzenia warunku źródłowego.
  19. Użytkownik powinien mieć możliwość zbadania alarmu bez jego potwierdzenia.
  + Dla zapewnienia odpowiedniego poziomu bezawaryjności serwera musi zostać zapewniona:

1. Dynamiczna rezerwa – możliwość natychmiastowej gotowości do przejęcia przez serwer zapasowy roli serwera podstawowego. Przełączenie awaryjne musi nastąpić w czasie krótszym niż 1 minuta bez działania użytkownika.
2. Redundancja na poziomie katalogów z konfiguracją - obsługa do pięciu (5) katalogów w trybie gotowości, ustawionych w kolejce, aby przejąć rolę działającego katalogu w sposób kaskadowy.
3. Katalog rezerwowy powinien synchronizować bazę danych konfiguracji z katalogiem podstawowym.
4. Samokontrola i automatyczna synchronizacja katalogów - katalogi rezerwowe mają obsługiwać scenariusze odzyskiwania po awarii, w których serwer może znajdować się w innym obszarze geograficznym (lub budynku) i przejmuje kontrolę tylko wtedy, gdy wszystkie katalogi o wyższym priorytecie przejdą w tryb offline. Katalogi rezerwowe mają obsługiwać synchronizację baz danych konfiguracji przy użyciu mechanizmu tworzenia kopii zapasowych i przywracania. Okres synchronizacji od kilkunastu minut do 1 tygodnia.
5. Katalog rezerwowy powinien obsługiwać synchronizację baz danych konfiguracji w czasie rzeczywistym za pomocą funkcji SQL Mirroring lub SQL Always On.

### Dodatkowe integracje z systemami zewnętrznymi

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:

* + 1. zewnętrzne systemy nadzoru wizyjnego,
    2. zewnętrzne systemy kontroli dostępu,
    3. integracja ALPR z kasami parkingowymi,
    4. systemy zarządzania budynkiem,
    5. środowisko kontroli dostępu (skaner identyfikatorów, synchronizacja kart, Guardtour),
    6. protokoły danych (modbus, BacNet, OPC, SNMP),
    7. ściana wizyjna,
    8. systemy zarządzania zasobami ludzkimi (HRMS).

## Kontrolery i urządzenia sterujące

Zakłada się zastosowanie wieloportowego kontrolera umożliwiającego na sterowanie co najmniej dwoma drzwiami podłączonymi bezpośrednio do płyty głównej oraz łącznie do max. 64 przejść kontrolowanych za pośrednictwem modułów rozszerzających.

Ze względu na konieczność obsługiwania dużej liczby poszczególnych elementów systemu, kontrolery muszą charakteryzować się natywną komunikacją oraz wysoką wydajnością, co umożliwi jego działanie niezależnie od liczby połączonych hostów aplikacji do kontroli dostępu. Konieczne jest, aby obsługiwały one protokół OSDP, bezpieczny OSDP, klawiatury, czytniki biometryczne, protokół Wiegand, Clock & Data, paski magnetyczne, F/2F i technologie czytnika F/2F.

Wymagane cechy techniczne, jakościowe i funkcjonalne kontrolerów:

* + zwiększone bezpieczeństwo zagwarantowane wbudowanym układem pamięci kryptograficznej i szyfrowaniem danych zapewniającym bezpieczną warstwę ochrony poufnych danych,
  + obsługa protokołu OSDP umożliwiającego bezpieczną komunikację pomiędzy kontrolerem a czytnikiem,
  + ochronę komunikacji z hostem z wykorzystaniem standardów TLS 1.2/1.1 lub AES-256/128,
  + ochronę złącza rozszerzającego kontrolera przez szyfrowanie w AES (seria 3 SIO),
  + kontrola dostępu do sieci z wykorzystaniem standardu 802.1X,
  + wsparcie dla OpenSSL,
  + globalna funkcja „antipasspback” w trybie online oraz lokalna funkcja „antipasspback” w trybie offline w ramach jednego kontrolera,
  + w zależności od potrzeb, praca w trzech trybach – online, offline oraz mieszanym,
* w przypadku zastosowania dodatkowych elementów takich jak np. moduły rozszerzeń mogą one być rozmieszczone w bezpośredniej bliskości przejść kontrolowanych.

## Czytnik 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:

* zakres temperatur pracy: nie węższy niż od -31℃ do 65℃
* klasa środowiskowa IP65
* możliwość komunikacji za pomocą OSDP, Wiegand, Clock-and-Data
* współpraca z kartami 13,56 MHz:
* obsługa technologii MIFARE Classic, MIFARE DESFire EV1 i iCLASS
* zgodność z normami ISO14443A (MIFARE) CSN, ISO14443B CSN, ISO15693 CSN
* obsługa systemu FeliCa™4 CSN, CEPAS4 CSN or CAN

Dla zapewnienia odpowiedniego poziomu bezpieczeństwa instalowane czytniki kart zbliżeniowych muszą wspierać technologie dwukierunkowej wymiany kluczy szyfrowania. Czytniki kart zbliżeniowych powinny być kompatybilne z modelem danych Secure Identity Object™ (SIO) i wspierać poświadczenia Secure Identity Object™ (SIO) zbudowane w oparciu o otwarte standardy, niezależnie od formy nośnika, zapewniając bezpieczeństwo oraz prywatność danych. Poświadczenia SIO mogą znajdować się na dowolnej liczbie nośników, takich jak karty zbliżeniowe iCLASS Seos, iCLASS SE, MIFARE Classic oraz MIFARE DESFire EV1. Urządzenia będą certyfikowanym punktem końcowym (węzeł TIP) w infrastrukturze Trusted Identity PlatformTM (TIP) zapewniającym skalowalny, bezpieczny system dostarczania cyfrowych poświadczeń, który sprawdza, rejestruje i zapewnia obsługę zarządzania cyklem życia certyfikowanych punktów końcowych.

Zaprojektowane czytniki powinny gwarantować wysoki poziom bezpieczeństwa również poprzez ograniczenie możliwości wprowadzenia niepożądanych zmian konfiguracji. Urządzenia powinny korzystać z bezpiecznego modelu zarządzania konfiguracją w oparciu o licznik konfiguracji oraz specjalne karty konfiguracyjne korzystając z bezpiecznego elementu (Secure Element) w celu ochrony kluczy oraz funkcji kryptograficznych zgodnego z międzynarodowym standardem Evaluation Assurance Level (EAL) na poziomie EAL 5+. Dla realizacji tak wysokiego poziomu bezpieczeństwa czytnik powinien umożliwiać konfigurację funkcji Velocity Checking (kontrola prędkości danych) w celu zabezpieczenia przed atakami elektronicznymi, opartymi na wielokrotnych próbach uwierzytelnienia.

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

* + 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.
  + 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.
  + 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. Karty użyte w projekcie są w standardzie wymiarów kart kredytowej i mają symbol 5006-PGGMN.

## 6. 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.

### 6.1 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. 5 lat gwarancji.

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).

### 6.2 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.

### 6.3 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:

* Zintegrowany multi-technologiczny czytnik zbliżeniowy z możliwością odczytu:

1. numerów seryjnych procesorów kart Mifare Classic/Mifare Plus/Mifare DESFire CSN (ISO 14443A) lub danych z sektorów pamięci;
2. numerów seryjnych kart iCLASS/iCLASS SE CSN (ISO 15693)/iCLASS Seos lub danych z sektorów pamięci;
3. szyfrowanych danych w standardzie SIO (Secure Identity Object)
   * Dostępny tryb pracy typu office (dwukrotne przyłożenie transpondera otwiera drzwi na stałe i ponowne dwukrotne przyłożenie zamyka na stałe.
   * 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).
   * Komunikacja z systemem kontroli dostępu powinna być realizowana z wykorzystaniem protokołu TCP/IP, a autoryzacja przeprowadzana przez system KD
   * Luźna klamka zewnętrzna - klamka wewnętrzna zasprzęglona na stałe (swobodne wyjście)
   * Możliwość przechowywania w pamięci minimum 10 awaryjnych kart (używanych wyłącznie w przypadku utraty komunikacji z anteną radiową/kontrolerem drzwiowym)
   * Diody LED do wizualizacji stanu pracy.
   * Odległość odczytu do 40mm w zależności od zastosowanej technologii zbliżeniowej
   * Zgodność z IP 52 (drzwi wewnętrzne) oraz IP54 (drzwi zewnętrzne)
   * Wymiary nie przekraczające 315 x 45 x 10/20 mm (H x W x D)
   * Standard radiowy IEEE 802.15.4 (2.4 GHz)
   * Szyfrowanie (komunikacja radiowa) 128 bitów AES
   * Zakres temperatur pracy od 0°C do 60°C
   * Dopuszczalna grubość drzwi od 40 do 100 mm
   * Zasilanie bateryjne – żywotność nie mniej jak 30 000 cykli
   * 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:

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

## 7. Urządzenia sieciowe

Do obsługi komunikacji wszystkich urządzeń systemu kontroli dostępu z wykorzystaniem protokołu TCP/IP, Wykonawca dostarczy i zainstaluje we wskazanych, ujętych w projekcie, węzłach sieci komputerowej Zamawiającego, dedykowane przełączniki sieciowe spełniające wymagania zawarte w załączniku nr 8 do SIWZ „Przełączniki sieciowe”.

## 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 12 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.