Załącznik Nr 2a do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest modernizacja systemu kontroli dostępu funkcjonującego w budynkach Naczelnego Sądu Administracyjnego przy ul. Gabriela Piotra Boduena 3/5, przy ul. Jasnej 2/4 oraz przy ul. Jasnej 6 w Warszawie, zwanych dalej również „obiektami NSA" lub „budynkami NSA".

Modernizacja systemu kontroli dostępu funkcjonującego we wszystkich budynkach NSA ma na celu ujednolicenie funkcjonujących obecnie systemów, usprawnienie nadzoru nad ich funkcjonowaniem, naprawami i serwisowaniem, aby zapewnić: kontrolę ruchu osobowego poprzez ograniczenie dostępności do pomieszczeń i/lub określonych stref w poszczególnych budynkach NSA, bezpieczeństwo pracowników i innych osób przebywających na terenie budynków NSA, ochronę mienia, zachowanie w tajemnicy informacji NSA, których ujawnienie mogłoby narazić Sąd na szkodę.

I. Informacja o obiektach:

1) Obiekt przy ul. Boduena 3/5:

   obiekt o powierzchni całkowitej około 14 600 m². Budynek biurowy, murowany, dwunastokondygnacyjny (10 kondygnacji naziemnych i 2 kondygnacje podziemne) – skrzydła zachodnie i wschodnie – oraz ośmiokondygnacyjny w części środkowej. Istniejący system SKD: Andover continuum. System sygnalizacji pożarowej: ESSER, WINMAG, POLON-ALFA, ITO.

2) Obiekt przy ul. Jasnej 2/4:

   obiekt o powierzchni całkowitej około 9500 m². Budynek biurowy, murowany, siedmiokondygnacyjny (6 kondygnacji naziemnych i 1 kondygnacja podziemna). Istniejący system SKD: Aritech ADVISOR MASTER; system sygnalizacji pożarowej SCHRACK.

3) Obiekt przy ul. Jasnej 6:

   obiekt o powierzchni całkowitej około 6 900 m², pełniący funkcję biurowo – administracyjną z programem zaplecza konferencyjno – szkoleniowego dla pracowników. Budynek murowany, jedenastokondygnacyjny, podpiwniczony. Istniejący system SKD: Bosch. System sygnalizacji pożarowej BOSCH, POLON-ALFA. Budynek wpisany jest do ewidencji zabytków Stołecznego Konserwatora Zabytków, lecz nie podlega ochronie konserwatorskiej w myśl ustawy z dnia 23 lipca 2003 r. o ochronie zabytków i opiece nad zabytkami (t.j.: Dz.U. z 2021 r., poz. 710 ze zm.).

II. Przewidywany zakres prac

Przewidywany zakres prac obejmuje modernizację systemu kontroli dostępu wraz z pracami towarzyszącymi zgodnie z projektem udostępnionym przez Zamawiającego na etapie wizji lokalnej, w tym:

1) Demontaż i przekazanie do magazynu Zamawiającego istniejących urządzeń systemu kontroli dostępu, które Zamawiający wskaże jako przeznaczone do zachowania.
2) Demontaż i utylizacja pozostałych urządzeń systemu kontroli dostępu (nieprzewidzianych przez Zamawiającego do dalszego użytkowania lub zachowania), zdemontowanego zbędnego okablowania i tras kablowych.
3) Budowa tam gdzie to niezbędne nowego okablowania i tras kablowych.
4) Dostawa, zainstalowanie, zaprogramowanie, uruchomienie i testy nowych urządzeń.
5) Przywrócenie pomieszczeń i terenu do stanu poprzedniego.
6) Zintegrowanie Systemu SKD z istniejącym systemem dźwigów osobowych (w budynku przy ul. Jasnej 6).
7) Zintegrowanie Systemu SKD z istniejącymi systemami sygnalizacji alarmu pożarowego we wszystkich budynkach NSA.
8) Zintegrowanie Systemu SKD z istniejącym systemem „elektronicznej listy obecności” we wszystkich budynkach NSA;
9) Przetestowanie Systemu pod kątem poprawności działania.
10) Zainstalowanie i konfiguracja oprogramowania zarządzającego Systemem SKD dla obsługi recepcji oraz administratorów Systemu, na stanowiskach komputerowych dostarczonych przez Wykonawcę.
11) Zainstalowanie i konfiguracja oprogramowania wizualizacyjnego Systemu SKD dla ochrony oraz administratorów Systemu, na stacjach roboczych dostarczonych przez Wykonawcę.
12) Przekazanie Zamawiającemu wszystkich licencji, kluczy, haseł do zainstalowanego oprogramowania, stacji roboczych, serwerów itp..
13) Serwisowanie i konserwacja Systemu w okresie gwarancji, przy czym przeglądy serwisowe powinny się odbywać nie rzadziej niż raz w roku, chyba, że producent urządzeń zaleca częstsze przeglądy.
14) Bezpłatna aktualizacja oprogramowania zarządzającego oraz firmware urządzeń do najnowszych wersji w całym okresie gwarancji, niezwłocznie po pojawieniu się nowej wersji.
15) Przeszkolenie pracowników Zamawiającego (do 10 osób) z zakresu obsługi i eksploatacji nowego Systemu.
16) Wykonanie dokumentacji powykonawczej, uzgodnionej z rzeczoznawcą ds. ochrony przeciwpożarowej wraz z przekazaniem praw autorskich.

III. Wymagania ogólne dotyczące prowadzenia prac

1) Wszystkie prace powinny być wykonywane w taki sposób, aby nie były uciążliwe dla pracowników NSA oraz nie utrudniały pracownikom NSA czynności służbowych.

2) Wykonawca zobowiązany jest do systematycznego wywozu odpadów powstałych w trakcie realizowanych prac uwzględniając koszty z tym związane w ofercie.
3) Wykonawca ponosi odpowiedzialność za wyniki działalności w miejscu wykonywanych realizacji przedmiotu zamówienia w zakresie:
   a) organizacji prac,
   b) zabezpieczenia interesów osób trzecich,
   c) ochrony środowiska,
   d) warunków bezpieczeństwa pracy oraz ochrony przeciwpożarowej.
4) Koszty naprawy ewentualnych uszkodzeń wewnątrz obiektów NSA oraz na zewnątrz, w tym nawierzchni dróg, chodników, posadzek, powierzchni ściennych lub sufitowych ponosi Wykonawca.
5) Wyroby stosowane w trakcie wykonywania prac mają spełniać wymagania polskich przepisów prawa, a wykonawca będzie posiadał dokumenty potwierdzające, że zostały one wprowadzone do obrotu zgodnie z odpowiednimi przepisami i posiadają wymagane parametry. Zamawiający przewiduje bieżącą kontrolę wykonywanych prac.
6) Kontroli Zamawiającego będą w szczególności poddane:
   a) stosowane materiały i urządzenia, w odniesieniu do dokumentów potwierdzających ich dopuszczenie do obrotu oraz zgodności parametrów z wymaganiami projektu Systemu SKD udostępnionego przez Zamawiającego podczas wizji lokalnej,
   b) sposób wykonania prac w aspekcie zgodności wykonania z projektem Zamawiającego oraz warunkami umowy,
   c) urządzenia i oprogramowanie zarządzające, wchodzące w skład Systemu, pod względem jakościowym powinny spełniać wymagania zawarte w Kryteriach Certyfikacyjnych opartych o dokumenty normatywne:
      - PN-EN-50130-4 Systemy alarmowe - Kompatybilność elektromagnetyczna;
      - PN-EN 60839-11-15 i PN-EN 60839-11-26 Systemy kontroli dostępu dla klasy dostępu B i rozpoznania 2;
      - Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, (dyrektywa NIS 2);
      - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych – RODO, m.in. w zakresie anonimizacji danych osobowych.
   d) urządzenia wchodzące w skład Systemu, zasilane napięciem wyższym niż 24V AC/DC, powinny posiadać znak bezpieczeństwa B lub CE.

Uwaga:

1) Aktualnie pracujące systemy kontroli dostępu obsługujące budynki NSA muszą pozostać sprawne niezależnie od wykonywanych prac modernizacyjnych. Dopuszcza się krótkotrwałe wyłączenia pojedynczych przejść, zgodnie z harmonogramem prac, który

sporządzi Wykonawca i przekaże Zamawiającemu do akceptacji. Ponadto, każdorazowo wyłączenie przejścia wymaga akceptacji Zamawiającego.

2) Istniejące systemy kontroli dostępu są częścią zintegrowanych systemów bezpieczeństwa budynków NSA. Ich demontaż należy przeprowadzić w ścisłym uzgodnieniu z Zamawiającym tak, aby nie naruszyć funkcji tych systemów niezwiązanych z kontrolą dostępu.

IV. Opis projektowanego Systemu SKD

1) Systemem kontroli dostępu objęto pomieszczenia wskazane w projekcie Systemu SKD przez Zamawiającego. System składa się z:
   - 148 przejść (w tym dwa dźwigi osobowe).
2) Wszystkie przejścia zaprojektowano jako pracujące w klasie rozpoznania 2 i w klasie dostępu B.
3) Każde przejście jednostronne pracujące w klasie rozpoznania 2 i w klasie dostępu B należy wyposażyć w jeden czytnik kart zbliżeniowych po stronie niechronionej oraz przycisk wyjścia po stronie chronionej(wg. projektu 112 przejść).
4) Każde przejście dwustronne pracujące w klasie rozpoznania 2 i w klasie dostępu B należy wyposażyć w dwa czytniki kart zbliżeniowych(wg. projektu 34 przejścia).
5) Jako podstawowe czytniki zbliżeniowe przyjęto urządzenia umożliwiające rozpoznawanie użytkowników za pośrednictwem kart zbliżeniowych standardu HID Seos lub DesFire EV3 (4k).
6) Projektowany System SKD składa się z:
   a) kontrolerów SKD,
   b) elementów wykonawczych Systemu SKD – czytniki, elektrozaczepy, kontaktrony, przyciski ewakuacyjne, samozamykacze, tripody, bramki uchylne, brama wjazdowa, szlabany,
   c) serwera Systemu SKD z bazą danych,
   d) komputerowych stacji roboczych.
7) Kontrolery Systemu SKD:
   a) kontrolery sieciowe projektowanego Systemu Kontroli Dostępu w obiekcie należy zainstalować w dedykowanych obudowach wraz modułami rozszerzeń i elementami zasilania oraz akumulatorami.
   b) zaprojektowano kontrolery sieciowe:
      - Typ 1 - kontroler z zasilaczem, porty LAN, RS485(wg. projektu-24 szt.);
      - Typ 2 - kontroler z zasilaczem, port RS485(122 szt.);
      - Typ 3 - kontroler z zasilaczem dedykowany do obsługi wind (2 szt);
   c) lokalizację poszczególnych szafek pokazano w części rysunkowej z rzutami obiektów.
8) Elementy wykonawcze Systemu Kontroli Dostępu:
   a) należy wymienić wyeksploatowane istniejące elektrozaczepy i samozamykacze w drzwiach objętych kontrolą dostępu. Wszystkie prace z tym związane należy przeprowadzić tak, aby nie naruszyć warunków certyfikacji i/lub wydanych aprobat technicznych drzwi,
   b) w celu awaryjnego otwarcia drzwi każde przejście kontroli dostępu należy wyposażyć w ewakuacyjny przycisk otwarcia. Kontrole stanu wskazanych przez Zamawiającego przejść należy podłączyć do monitorujących kontrolerów drzwiowych,
   c) w obu portierniach istnieje zespół tripodów, bramek uchylnych i dodatkowych wygrodzeń, pełniących funkcję wejścia na teren obiektu osób upoważnionych. Bramki

uchylne podlegają wymianie, pozostałe urządzenia pozostają bez zmian. Wszystkie tripody i bramki należy zintegrować z nowoprojektowanym Systemem SKD.

9) Wytyczne instalacyjne – instalacja urządzeń:
   a) wszystkie urządzenia Systemu SKD należy montować zgodnie z instrukcją instalacji oraz dokumentacją techniczno-ruchową danego urządzenia. W miarę możliwości nowe urządzenia należy montować w miejscach, w których były zamontowane urządzenia istniejących systemów,
   b) przy instalacji urządzeń należy uwzględnić wszystkie wymagania producenta danego urządzenia oraz wytyczne:
      - głowice czytające należy instalować tak, aby ich górna krawędź znajdowała się ok.1,4 m od podłoża a odległość od futryny w miarę możliwości architektonicznych nie przekraczała 20 cm;
      - przycisk ewakuacyjny należy zainstalować w bezpośrednim sąsiedztwie głowicy lub przycisku wyjścia po stronie chronionej tak, aby ich górna krawędź znajdowała się ok.1,4 m od podłoża;
      - przycisk wyjścia należy zainstalować w bezpośrednim sąsiedztwie głowicy po stronie chronionej pod przyciskiem ewakuacyjnym w osi centralnej przycisku, a odległość od futryny w miarę możliwości architektonicznych nie przekraczała 20cm;
      - nowo montowaną czujkę magnetyczną - stykową, pełniącą rolę czujnika otwarcia, należy montować przy górnej krawędzi skrzydeł drzwiowych w odległości 2/3 od zawiasów. W istniejących przejściach czujki należy zamontować w poprzednio montowanych miejscach.
10) Wytyczne instalacyjne – okablowanie:
   a) zamawiający dopuszcza wykorzystanie, tam gdzie to możliwe, istniejącego okablowania. Wykonawca jest zobowiązany do wykonania pomiarów potwierdzających możliwość wykorzystania istniejącego okablowania (wymagany jest pomiar rezystancji izolacji oraz ciągłości żył),
   b) wszystkie nowo instalowane kable i przewody układane wewnątrz budynków powinny mieć klasę reakcji na ogień min. B2ca,
   c) podłączenie kontrolera sieciowego SKD do sieci LAN należy wykonać kablem UTP kat.6,
   d) połączenie czytnika kart zbliżeniowych z kontrolerem drzwiowym należy wykonać przewodem do transmisji danych wykonanym w klasie B2ca np. BiTsensorPE(St)CH B2ca,
   e) połączenie pomiędzy elementami wykonawczymi SKD (zwory elektromagnetyczne i elektrozaczepy), a kontrolerem drzwiowym należy wykonać kablem N2XH-J 2x1. Połączenie to należy wykonać przez przycisk ewakuacyjny,
   f) połączenie pomiędzy stykiem monitorowania przycisku ewakuacyjnego i czujnikiem otwarcia a kontrolerem drzwiowym należy wykonać kablem UTP kat.5e B2ca,
   g) przed uruchomieniem instalacji należy wykonać badania polegające na sprawdzeniu:
      - poprawności połączeń;
      - umocowania połączeń;
      - właściwej numeracji elementów;
      - adresów i oznakowania elementów;
      - właściwego oprogramowania Systemu.
   h) Uruchomienie Systemu należy wykonać zgodnie z instrukcją instalacji systemu dostarczoną przez Wykonawcę.

11) Sieć LAN systemów bezpieczeństwa:
    a) transmisja danych odbywać się będzie w oparciu o fizycznie wydzieloną sieć Ethernet. Sieć transmisyjna powinna zostać wykonana w topologii gwiazdy z centralnym węzłem w postaci istniejącego w budynku Boduena 3/5, Głównego Punktu Dystrybucyjnego (GPD-CCTV) oraz punktami pośrednimi w postaci szaf wiszących. Połączenie urządzeń aktywnych pomiędzy Punktami LPD i Głównym Punktem Dystrybucyjnym (GPD) powinno zostać wykonane przy wykorzystaniu połączeń światłowodowych jednomodowych,
    b) podłączenie serwera do sieci LAN należy wykonać dedykowanym kablem krosowym UTP kat.6,
    c) połączenie kontrolera SKD (z portem LAN) z przełącznikiem sieciowym LAN należy wykonać kablem UTP kat.6. Należy wykonać dedykowane połączenie pomiędzy kamerą, a przełącznikiem sieciowym. Długość jednego odcinka nie może przekraczać 90m,
    d) dla stanowisk nadzoru Systemu należy wykonać dedykowane gniazda RJ45 kat. 6 wydzielonej sieci LAN systemu bezpieczeństwa,
    e) przewody UTP będą układane w następujący sposób:
        - w budynku - na istniejących trasach kablowych. W przypadku braku tras kablowych, należy ułożyć dodatkowe korytka kablowe;
        - w istniejącej kanalizacji teletechnicznej.
12) Wymagania dla okablowania strukturalnego:
    a) system okablowania strukturalnego ma zapewnić niezawodną i wydajną warstwę fizyczną sieci teleinformatycznej, która zagwarantuje wystarczający zapas parametrów transmisyjnych dla działanie dzisiejszych i przyszłych aplikacji transmisyjnych. W celu spełnienia najwyższych wymogów jakościowych i wydajnościowych należy zapewnić:
        - okablowanie miedziane spełniające wymagania kategorii 6 (klasy E);
        - okablowanie skrętkowe w wersji nieekranowanej;
        - certyfikaty wydane przez międzynarodowe, renomowane niezależne laboratorium badawcze np. Delta, potwierdzające zgodność okablowania miedzianego z najnowszymi, aktualnymi normami okablowania strukturalnego ISO/IEC 11801:2011 (która zastępuje normy ISO/IEC 11801:2002, ISO/IEC 11801 AMD1:2006, ISO/IEC 11801 AMD2:2010), EN 50173-1:2011, TIA-568-C.2. Należy zapewnić certyfikaty potwierdzające zgodność z normami w zakresie testu całego łącza oraz niezależnych komponentów (kabel, panel, złącze RJ45). Nie dopuszcza się certyfikatów z lokalnych instytutów łączności, ponieważ nie posiadają one wystarczających akredytacji do testów wszystkich parametrów wymienionych w powyższych normach.
13) Pomiary okablowania miedzianego:
    a) wszystkie łącza skrętkowe w Systemie należy przetestować pod kątem spełniania wymogów klasy E / kategorii 6 wg ISO 11801 lub EN 50173,
    b) należy przeprowadzić pomiary w układzie pomiarowym typu „Permanent Link” (bez kabli krosowych),
    c) pomiary należy wykonać miernikiem o poziomie dokładności, co najmniej „Level IV”. Zalecane typy mierników: DSX-5000, DTX-1800 lub DTX-1200 firmy Fluke Networks,
    d) należy wykonać pomiary certyfikacyjne, w których po zmierzeniu rzeczywistych wartości parametrów łącza, miernik automatycznie porówna je z granicznymi wartościami definiowanymi przez aktualne normy okablowania i określi wynik porównania,

e) wyniki pomiarów certyfikacyjnych wszystkich łączy muszą być prawidłowe,
f) pomiary należy wykonać zgodnie z wymaganiami normy PN-EN 50346,
g) wymagany zakres mierzonych parametrów dla każdej z par (kombinacji par):
   - mapa połączeń - poprawność i ciągłość wykonanych połączeń;
   - straty odbiciowe (ang. RL - Return Loss);
   - straty wtrąceniowe - tłumienie (ang. IL - Insertion Loss);
   - straty przesłuchów zbliżnych (ang. NEXT - Near End Crosstalk Loss);
   - sumaryczny parametr NEXT (ang. PSNEXT – Power Sum NEXT);
   - współczynnik tłumienia w odniesieniu do straty przesłuchu na bliskim końcu (ang. ACR-N – Attenuation to Crosstalk Ratio at the Near end);
   - sumaryczny współczynnik ACR-N (ang. PSACR-N – Power Sum ACR-N);
   - współczynnik tłumienia w odniesieniu do straty przesłuchu na dalekim końcu (ang. ACR-F – Attenuation to Crosstalk Ratio at the Far end);
   - sumaryczny współczynnik ACR-F (ang. PSACR-F – Power Sum ACR-F);
   - rezystancja pętli dla prądu stałego (ang. DC current loop);
   - opóźnienie propagacji (ang. Propagation delay);
   - różnica opóźnień propagacji (ang. Delay skew).

14) Zasilanie podstawowe.
   a) należy wykorzystać istniejące wydzielone obwody zasilające istniejących urządzeń SKD.
   b) stacje robocze, serwer, bramki uchylne zasilić z istniejących obwodów zasilających.
15) Zasilanie rezerwowe.
   a) po zaniku podstawowego zasilania sieciowego każdy kontroler (sterownik) powinien automatycznie przełączyć się na pracę ze źródła zasilania rezerwowego (akumulator), które powinno gwarantować pracę ciągłą całego osprzętu przejścia kontrolowanego:
      - przez co najmniej przez 12 godzin, w przypadku przejścia wyposażonego w zworę elektromagnetyczną;
      - przez co najmniej 12 godzin, w przypadku przejścia wyposażonego w rygiel elektromagnetyczny rewersyjny lub elektro-zaczep rewersyjny.
   b) Wykonawca jest zobowiązany do złożenia Zamawiającemu obliczeń potwierdzających prawidłowość doboru akumulatorów.

V. Wymagania dla Systemu i urządzeń.

1) Identyfikacja osób i pojazdów w Systemie SKD:
   a) elementy identyfikujące użytkownika - identyfikatory zbliżeniowe (karty, breloki) powinny być oparte o bezpieczną technologię, wybraną z poniżej dopuszczalnych:
      - DesFire EV3 (4k);
      - HID SEOS ®;
      - Idesco.
   b) identyfikator zbliżeniowy powinien posiadać, zakodowany w procesie produkcji, unikalny identyfikacyjny numer seryjny (CSN - Custom Serial Number). Identyfikator ten musi też posiadać możliwość zapisu na nim, przez administratora Systemu za pomocą dedykowanego programatora identyfikatorów, własnego, prywatnego kodu identyfikacyjnego z wykorzystaniem bezpiecznych pól pamięci identyfikatora o zaszyfrowanej treści (zawartości pól pamięci) oraz zaszyfrowanym dostępie do nich. Szyfrowanie winno wykorzystywać algorytm AES z kluczem 128 bitowym lub wyższym,

c) nadruk widoczny na identyfikatorze, nie może być bezpośrednią reprezentacją prywatnego kodu identyfikacyjnego, zaprogramowanego w identyfikatorze,
d) programator identyfikatorów oraz prywatne klucze szyfrujące powinny pozostawać w wyłącznym posiadaniu właściciela Systemu. Stanowisko programatora powinno być wydzielone od reszty Systemu i wyposażone w dedykowany, zabezpieczony komputer (laptop). Programator wraz z dedykowanym mu komputerem powinien być przechowywany w sposób bezpieczny (zamykana szafa pancerna lub sejf), w bezpiecznym miejscu i udostępniany osobom uprawnionym (administrator Systemu) tylko na czas programowania (kodowania) identyfikatorów,
e) czytniki identyfikatorów powinny zapewniać szyfrowaną komunikację bezprzewodową z identyfikatorami, powinny zapewniać odczyt danych z wybranego pola pamięci oraz odszyfrowanie z tych danych prywatnego kodu identyfikacyjnego użytkownika,
f) czytnik powinien być zabezpieczony przed odczytem identyfikatorów pracujących w innych technologiach (karty płatnicze, NFC), powinien odczytywać jedynie identyfikatory zaprogramowane przez właściciela Systemu,
g) czytniki identyfikatorów powinny zapewniać szyfrowaną komunikację z urządzeniami decyzyjnymi przejść (kontrolerami przejść), wykorzystującą protokół OSDPv2 (Open Supervised Device Protocol), opierający się na komunikacji LAN,
h) klucz szyfrujący, wykorzystywany do komunikacji z czytnikami nie może być kluczem fabrycznym czytnika (SCBK-D). Podczas wdrożenia musi zostać zaimplementowany unikalny klucz prywatny,
i) System winien obsługiwać następujące rodzaje czytników:
   - zbliżeniowe bez klawiatury numerycznej;
   - zbliżeniowe z klawiaturą numeryczną (w celu podwójnej weryfikacji tożsamości użytkownika za pomocą kodu identyfikatora i informacji zapamiętanej (kod karty + PIN) lub rejestracji szczególnych zdarzeń RCP);
   - zbliżeniowe, bezprzewodowe, zasilane bateryjnie (czytnik zintegrowany z zamkiem drzwi);
   - przenośne pulpity ręczne z czytnikami zbliżeniowymi, przeznaczone dla służb ochrony w celu weryfikacji tożsamości osób przebywających na terenie obiektu;
   - czytniki pilotów zdalnego sterowania zintegrowane z Systemem SKD;
   - kamery ANPR jako czytniki tablic rejestracyjnych samochodów, min 3 numery tablic dla każdego użytkownika parkingu.

2) Komunikacja i przesyłanie danych w Systemie SKD:
   a) w zaprojektowanym Systemie SKD komunikacja na odcinkach wskazanych poniżej, powinna być szyfrowana zgodnie ze wskazanymi kryteriami:
      - identyfikator (karta zbliżeniowa) – czytnik: szyfrowana komunikacja bezprzewodowa, odczyt kodu identyfikacyjnego z identyfikatora, z pola pamięci o zaszyfrowanym dostępie do jego zawartości;
      - czytnik – kontroler SKD: szyfrowana komunikacja, wykorzystującą protokół OSDPv2 (Open Supervised Device Protocol), opierający się na algorytmie szyfrowania danych AES z kluczem 128 bitów. Klucz szyfrujący, wykorzystywany do komunikacji z czytnikami nie może być kluczem fabrycznym czytnika (SCBK-D). Podczas wdrożenia musi zostać zaimplementowany i wykorzystywany w komunikacji unikalny klucz prywatny;
      - kontrolery SKD – serwer SKD: szyfrowana komunikacja z wykorzystaniem protokołu TCP/IP lub UDP/IP, gdzie przesyłane dane są zaszyfrowane algorytmem AES z kluczem szyfrującym o minimalnej długości 128 bitów.

3) Wymagane cechy funkcjonalne oprogramowania Systemu SKD:
   a) oprogramowanie zarządzające Systemu SKD powinno w szczególności zapewniać realizację następujących funkcji i posiadać poniższe cechy:
      - praca rozproszona Systemu w sieciach LAN / WAN z jednolitym zarządzaniem elementami Systemu rozmieszczonymi w różnych punktach i obsługą dowolnej liczby obiektów (biura, oddziały).
      - obsługa minimum 200 przejść kontrolowanych – kontrolerów przejść, z możliwością jego rozbudowy o kolejne przejścia kontrolowane.
      - obsługa pracy urządzeń SKD w minimum 50 lokalizacjach zdalnych sieci LAN/WAN tj. obsługiwać minimum 50 adresów IP sieci (w wydzielonych obiektach, budynkach lub fragmentach budynków).
   b) System powinien posiadać możliwość rozbudowy pojemności do minimum 5000 użytkowników'
   c) oprogramowanie powinno zapewnić skalowalność sprzętową i programową tj. zdolność do:
      - dodawania kolejnych urządzeń w celu rozbudowy Systemu;
      - dodawania oraz integracji urządzeń służących do dodatkowej identyfikacji użytkowników np. kamer rozpoznawania tablic rejestracyjnych;
   d) architektura oprogramowania winna wykorzystywać model klient – serwer gdzie:
      - serwer główny (centralna baza danych) i serwis komunikacyjny z kontrolerami SKD;
      - stacje klienckie (terminale) - od 2 do 100 stanowisk operatorskich w różnych lokalizacjach, w tym moduł obsługi dla osób odwiedzających – gości oraz zarządzania kluczami.
   e) System musi posiadać polski interfejs językowy oprogramowania,
   f) licencjonowanie i uwierzytelnianie poszczególnych komponentów oprogramowania odbywa się z wykorzystaniem lokalnego centralnego serwera licencji, obecnego w Systemie SKD,
   g) możliwość automatycznego upgrade'u komponentów oprogramowania Systemu SKD na stanowiskach klienckich (terminalach) przy wykorzystaniu technologii „click-once",
   h) uzupełnienie bazy użytkowników SKD w Systemie SKD o ich zdjęcia oraz wyświetlania tych zdjęć na ekranie monitora terminala, w dedykowanej aplikacji podglądu zdarzeń „on-line" w Systemie SKD, w pomieszczeniu ochrony/monitoringu, po użyciu identyfikatora (karty zbliżeniowej) na dowolnym czytniku w Systemie SKD,
   i) wielokrotnego importu bazy/listy danych osobowych pracowników z zewnętrznego źródła w postaci pliku tekstowego o ustalonym, wymaganym przez SKD formacie (przykład danych : imię, nazwisko, symbol, nr ewidencyjny, data urodzenia, uwagi, kod, miasto, kraj, pesel, dowód tożsamości, budynek, nr pokoju, tel. do pokoju, tel. komórkowy, tel. do sekretariatu, firma, dział, stanowisko, kategoria, płeć, tel. do domu, tel. do pracy, marka pojazdu, nr rejestracyjny, nazwa karty, kod karty, grupa KD, grupa RCP, karta ważna od, karta ważna do),
   j) każdy użytkownik Systemu powinien posiadać w nim co najmniej 2 kody identyfikatorów (identyfikator podstawowy + identyfikator dodatkowy),
   k) definiowanie okresu ważności karty, po którym karta jest automatycznie dezaktywowana,
   l) personalizacji (projektowania) i drukowania kart/identyfikatorów pracowniczych, gości, przepustek z poziomu oprogramowania zarządzającego SKD, z wykorzystaniem specjalizowanej drukarki do kart z wykorzystaniem technologii termo-sublimacji;

wyklucza się wykorzystywanie odrębnego oprogramowania do nadruku na identyfikatorach z odrębną bazą danych z projektami i danymi do nadruku,

m) w projektach identyfikatorów pracowników wykorzystane muszą być następujące dane zawarte w bazie Systemu SKD:
   - na awersie: imię, drugie imię, nazwisko, firma, dział, stanowisko, numer ewidencyjny, kategoria, nr karty, data ważności, tytuł/stopień, zdjęcie osoby, obraz (dodatkowy obrazek, widok itp.), logo, tło karty (jednolity kolor, obraz z pliku .jpg.);
   - na rewersie: cztery niezależne pola informacyjne, logo i tło karty (jednolity kolor, obraz z pliku .jpg.)
n) w projektach identyfikatorów dla interesantów wykorzystane muszą być następujące dane zawarte w bazie Systemu SKD:
   - na awersie: nr karty, data ważności, obraz (dodatkowy obrazek, widok itp.), logo, tło karty (jednolity kolor, obraz z pliku .jpg.);
   - na rewersie: cztery niezależne pola informacyjne, logo i tło karty (jednolity kolor, obraz z pliku .jpg.)
o) ręczne lub automatyczne usuwanie danych osobowych o pracownikach i gościach zarejestrowanych w Systemie SKD i ewidencji gości, ręczna lub automatyczna anonimizacja danych osobowych; funkcjonalność uwzględniająca wymogi Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych,
p) tworzenie w Systemie SKD grup i podgrup dostępowych, zorganizowanych w formie wieloelementowego drzewa celem grupowego lub indywidualnego nadawania uprawnień dostępowych dla wybranych użytkowników lub grup. W ramach drzewa grup dostępowych musi funkcjonować mechanizm dziedziczenia nadanych uprawnień dostępowych w relacjach: grupa dostępowa nadrzędna – grupa podrzędna (podgrupa) oraz grupa dostępowa – członek grupy dostępowej,
q) wykorzystywanie dostępowych schematów czasowych w postaci kalendarzy/harmonogramów rocznych lub tygodniowych z definicjami dozwolonych przedziałów dostępu z dokładnością do godzin i minut (w każdym kalendarzu/harmonogramie w każdym dniu możliwy co najmniej 1 przedział; przedziały mogą być różne),
r) wykorzystania w odniesieniu do wybranych obszarów kontrolowanych zaawansowanych funkcji dostępu warunkowego w postaci:
   - funkcja kontroli naprzemienności zdarzeń wejście-wyjście tj. "anti-passback" globalny, wymuszająca na użytkownikach konieczność naprzemiennego używania identyfikatorów na wejściu i wyjściu do/z obszaru oraz blokująca możliwość wielokrotnego użycia identyfikatora w tym samym kierunku „pod rząd” (np. po pierwszym „wejściu” próba kolejnego „wejścia” bez wcześniejszego „wyjścia”);
   - funkcja udzielenia dostępu do obszaru (pomieszczenia) o ile znajduje się w nim jego właściciel;
   - funkcja ograniczania liczby osób jednocześnie przebywających w obszarze (pomieszczeniu) do zadanej wielkości maksymalnej; odmowa dostępu osobom uprawnionym, jeśli ich wpuszczenie oznaczałoby przekroczenie zadanego limitu osób;
   - blokowanie ruchu do/z obszaru kontrolowanego osoby uprawnionej w związku z działaniem funkcji „losomatu” losującej osoby do kontroli osobistej lub kontroli bagażu;

- Możliwość ustawiania różnego prawdopodobieństwa wylosowania dla poszczególnych grup lub osób.

s) manualne odblokowywanie (do odwołania), dowolnego przejścia (drzwi, kołowrót, bramka uchylna), uprawnionym identyfikatorem (karta, brelok, tag); Opcja automatycznego przywrócenia przejścia do stanu spoczynku o wybranej godzinie,
t) automatyczne blokowanie i odblokowanie wybranych drzwi z poziomu oprogramowania zarządzającego w:
   - ustalonym, wcześniej zadanym okresie;
   - ustalonych, wcześniej zadanych dniach tygodnia;
   - ustalonym przedziale czasowym (godzinach);
u) awaryjnego otwierania grup przejść przez operatora Systemu przy użyciu uprzednio przygotowanych scenariuszy ewakuacyjnych (użycie zdefiniowanego przycisku w programie zarządzającym może spowodować odblokowanie szeregu przejść w ciągu drogi ewakuacyjnej),
v) integracji Systemu SKD z systemem windy zapewniającej sterowanie dostępem do przycisków wyboru pięter w kabinie windy, umożliwiającej przyznawanie dostępu wybranym osobom do poszczególnych pięter budynku (czytnik + przyciski w kabinie windy); realizacja tej funkcjonalności uzależniona od typu sterownika windy,
w) możliwość realizacji tzw. "układu śluzy", czyli takiego sprzężenia kontrolerów, aby w danej chwili tylko jedne drzwi ze sprzężonych przejść kontrolowanych mogły być otwarte; wówczas próby przejścia osób uprawnionych przez pozostałe przejścia sprzężone zostaną zablokowane,
x) generowanie dodatkowych reakcji Systemu na zaistniałe w nim zdarzenia np. dźwięk, komunikat tekstowy, wyświetlenie symbolu graficznego na ekranie,
y) podgląd ruchu osobowego na wybranych przejściach lub w całym Systemie, w trybie on-line. Dla wybranych typów zdarzeń (alarmowych) oraz przejść, możliwa dodatkowa reakcja w postaci komunikatów ostrzegawczych dla służb ochrony,
z) generowanie raportów dotyczących zaistniałych w Systemie zdarzeń z filtracją według ustalonych kryteriów oraz możliwością ich wydruku lub eksportu do pliku tekstowego „*.csv” i wyświetlania na ekranie w formie tabeli,
aa) wykonywania archiwalnych raportów stanu obecności osób w obszarach kontrolowanych w dowolnie wybranym punkcie czasowym z możliwością śledzenia korelacji między czasem przebywania a uprawnieniami dostępu osób,
bb) podglądu ON LINE listy osób aktualnie przebywających w obiekcie,
cc) tworzenie raportów ewakuacyjnych z prezentacją:
   - ostatniej lokalizacji pracowników oraz zarejestrowanych gości, obecnych na terenie obiektu (na podstawie rejestracji zdarzeń w kontrolerach Systemu);
   - liczby osób uprawnionych do dostępu;
   - liczby osób obecnych w chwili generowania raportu;
   - daty, godz. wykonania raportu.
dd) rejestracji i rozliczania czasu pracy pracowników (użytkowników) w oparciu o karty i czytniki funkcjonujące w Systemie SKD (jako możliwość rozbudowy Systemu SKD o moduł RCP wraz ze stosownym poszerzeniem funkcjonalności zintegrowanego oprogramowania zarządzającego SKD),
ee) udostępnianie indywidualnych raportów RCP dla każdego pracownika przez przeglądarkę internetową przy wykorzystaniu indywidualnych loginów i haseł,
ff) obecność funkcji (modułu) ewidencjonowanej obsługi ruchu innych osób przebywających do Sądu (interesanci) wraz z tworzeniem bazy danych osób

odwiedzających obiekt (interesantów) oraz administrowania ich kartami dostępowymi (baza danych o interesantach musi być integralną częścią bazy SKD),

gg) obsługi skanera (czytnika) dokumentów tożsamości - dowodów osobistych lub paszportów, w celu przyspieszenia procesu rejestracji osób odwiedzających (skanowanie polega na odczycie z dokumentu wybranych pól tekstowych – np. numer dowodu, bez przechowywania obrazu dokumentu),

hh) definiowania kart dla interesantów, kart jednodniowych,

ii) współpraca z wrzutnią grawitacyjną dla kart interesantów celem usprawnienia obsługi ruchu osób odwiedzających, automatycznie wyrejestrowującą wizytę gościa (koniec wizyty); automatyczne odbieranie kart gościnnych,

jj) wykonywanie raportów z pobytów interesantów na terenie obiektu, ich wydruku oraz eksportu do pliku (csv),

kk) obecność funkcji tzw awizacji gości do awizowania przez przeglądarkę internetową (zgłaszanie, przez osoby uprawione, do Systemu SKD, oczekiwanych gości); zgłoszenia dokonane widoczne w aplikacji do obsługi gości w recepcji celem dalszych działań recepcjonisty zgodnie z procedurą obsługi ruchu gości),

ll) obecność funkcji (modułu) zarządzania dostępem pracowników zdefiniowanych SKD do zdefiniowanych Systemie SKD kluczy do pomieszczeń nie objętych SKD. Wspomaganie recepcjonisty/ochrony w procesie wydawania i odbioru kluczy, rejestracja zdarzeń wydania (pobrania) i zwrotu (zdania) klucza. Wykonywanie stosownych raportów, ich wydruk, eksport w formacie HTML lub Excel (csv),

mm) możliwość integracji z Active Directory (uwierzytelnianie logowania do aplikacji będących komponentami oprogramowania SKD z poświadczeniami LDAP),

nn) możliwość współpracy z elektronicznymi licznikami, prezentującymi w czasie rzeczywistym stan osobowy w określonych strefach obiektu,

oo) integracja z platformami wizualizacji systemów bezpieczeństwa BMS (KD, CCTV, SSWiN, PPOŻ, DSO), wizualizacja 2D lub 3D,

pp) możliwość indywidualnego dostosowania Systemu SKD do wymogów Zamawiającego na podstawie odrębnych uzgodnień i specyfikacji.

4) Wymagane cechy urządzeń sterujących (kontrolerów) Systemu SKD:

a) urządzenia decyzyjne (kontrolery przejść) powinny być wyposażone we wbudowany (zintegrowany) interfejs RS485 do podłączenia czytników, obsługujących protokół OSDPv2. Interfejs ten powinien zapewniać stały monitoring pracy podłączonych do niego czytników z możliwością wykrywania prób sabotażu, takich jak: zdjęcie czytnika ze ściany lub utrata komunikacji z czytnikiem,

b) urządzenia decyzyjne (kontrolery przejść), współpracujące z czytnikami kart oraz pozostałymi elementami osprzętu kontroli dostępu (zamki elektryczne, zwory, rygle, elektrozaczepy, brama, szlabany, tripody, kołowrotki, bramki, przyciski, czujniki stanu drzwi itp.) powinny posiadać możliwość pracy zarówno w trybie komunikacji ciągłej z serwerem SKD (tryb „ON-LINE") oraz w trybie autonomicznym, gdy brak jest połączenia z serwerem SKD (tryb „OFF-LINE"),

c) przy zaniku podstawowego zasilania sieciowego (230V AC) kontrolery przejść powinny zapewniać ciągłość swojej pracy oraz pracy czytników, przy wykorzystaniu akumulatorowego podtrzymania zasilania,

d) przejście kontrolera przejścia z trybu pracy „ON-LINE" w tryb „OFF-LINE" powinno odbywać się automatycznie,

e) praca w trybie autonomicznym („OFF-LINE") każdego kontrolera przejścia powinna zapewniać:

- możliwość przechowania w jego pamięci nieulotnej uprawnień dostępowych dla min. 8000 użytkowników (identyfikatorów);
- możliwość zapisu min. 16000 zdarzeń w pamięci nieulotnej w zorganizowanym buforze okrężnym każdego kontrolera.

f) każdy kontroler przejścia powinien być wyposażony w pamięć stronicowaną, umożliwiającą przesyłanie do niego kompletu nowych nastaw dla kontrolera przy jednoczesnym zapewnieniu ciągłej, niezakłóconej pracy kontrolowanego przezeń przejścia według poprzednich nastaw. Po odebraniu kompletu nowych nastaw z serwera SKD, kontroler powinien przełączyć się do pracy z nowymi nastawami w sposób automatyczny.
g) każdy kontroler powinien być wyposażony w zintegrowany rozdzielacz wewnętrznej magistrali transmisyjnej, dla połączenia transmisyjnego danych pomiędzy kontrolerami, na minimum dwie gałęzie,
h) po zaniku podstawowego zasilania sieciowego każdy kontroler (sterownik) powinien automatycznie przełączyć się na pracę ze źródła zasilania rezerwowego (akumulator), które powinno gwarantować pracę ciągłą całego osprzętu przejścia kontrolowanego:
   - przez co najmniej przez 12 godzin, w przypadku przejścia wyposażonego w zworę elektromagnetyczną;
   - przez co najmniej 12 godzin, w przypadku przejścia wyposażonego w rygiel elektromagnetyczny rewersyjny lub elektrozaczep rewersyjny.
i) kontroler powinien automatycznie się wyłączyć po osiągnięciu przez akumulator najniższego dopuszczalnego poziomu napięcia, a następnie automatycznie wznowić pracę po przywróceniu podstawowego zasilania sieciowego NN230VAC. W przypadku, gdy przed wyłączeniem kontroler pracował z aktywnym połączeniem transmisyjnym z serwerem SKD (tryb „ON-LINE”), po przywróceniu podstawowego zasilania sieciowego powinno nastąpić automatyczne wznowienie pracy w tym samym trybie („ON-LINE”),
j) aby zagwarantować odpowiednie bezpieczeństwo i niezawodność działania Systemu w skali całego obiektu oraz spełnić polską normę PN-EN-60839-11-1:2024-01, kontrolery powinny nadzorować tylko jedno przejście kontrolowane bez względu na to, czy jest to przejście jednostronnie (jeden czytnik po stronie „wejściowej” albo „wyjściowej” przejścia) czy dwustronnie kontrolowane (dwa czytniki – jeden po stronie „wejściowej” a drugi po stronie „wyjściowej” przejścia) i niezależnie od tego jaki element blokujący (np. drzwi, tripod, bramka, szlaban) stanowi zaporę tego przejścia. Takie rozwiązanie winno być zastosowane w głównych wejściach do budynku. W przypadku przejść wewnętrznych wymaga się instalacji kontrolerów w strefach chronionych,
k) uszkodzenie lub próba sabotażu obwodu transmisji danych do/z kontrolera musi być bezwzględnie sygnalizowana na terminalu ochrony odpowiednim komunikatem alarmowym oraz rejestracją zdarzenia alarmowego w Systemie SKD,
l) obudowa kontrolera powinna zabezpieczać kontroler przed nieautoryzowanym dostępem osobom nieuprawnionym. Otwarcie obudowy powinno być sygnalizowane alarmem dla służb ochrony obiektu oraz rejestracją zdarzenia alarmowego w Systemie SKD,
m) kontrolery Systemu SKD powinny być podłączone do dedykowanej sieci Ethernet, gdzie komunikacja powinna wykorzystywać protokoły TCP/IP lub UDP/IP a przesyłane dane powinny być zaszyfrowane protokołem AES z kluczem o minimalnej długości 128 bitów,

n) kontroler powinien być wyposażony w dedykowane zaciski dla monitorowania przycisku ewakuacyjnego (PEP z sygnalizacją), umożliwiające odnotowanie momentu jego użycia oraz powrotu do stanu spoczynku,
o) oprogramowanie Systemu SKD powinno zapewniać możliwość zmiany, prywatnych kluczy szyfrujących (AES128) w kontrolerach SKD, centralnie z poziomu serwera Systemu SKD. Klucze te wykorzystywane będą do bezpiecznej komunikacji z czytnikami przy pomocy protokołu OSDPv2,
p) kontroler winien posiadać możliwość wyposażenia go w dodatkowe wejścia / wyjścia cyfrowe umożliwiające współpracę z innymi elementami bezpieczeństwa (np. czujki PPOŻ, dymu, kamery CCTV etc.),
q) wymagane cechy kamer ANPR (Automatic Number Plate Recognition) do identyfikacji tablic rejestracyjnych pojazdów,
r) wytyczne dla kamer ANPR rozpoznawania tablic rejestracyjnych, zainstalowanych przy wjeździe do parkingu podziemnego. Założono, że wyposażenie przejazdu w postaci 2 szlabanów oraz bramy segmentowej pozostaje bez zmian,
   - kamera ANPR powinna być zintegrowana z Systemem SKD w taki sposób, by rozpoznanie numeru rejestracyjnego pojazdu było tożsame z użyciem karty właściciela na czytniku wjazdowym/wyjazdowym. Skutkiem rozpoznania tablicy rejestracyjnej pojazdu winno być otwarcie szlabanu wjazdowego oraz bramy segmentowej,
s) kamera powinna posiadać możliwość konfiguracji strefy odczytu tablicy rejestracyjnej pojazdu oraz miejsca wyzwalania odczytu. Wyzwalanie odczytu tablicy rejestracyjnej powinno być konfigurowane dla wybranego kierunku ruchu pojazdu – zbliżania lub oddalania od kamery,
t) wyzwalanie odczytu numeru rejestracyjnego powinno być możliwe metodą alternatywną przez pobudzenie wejścia cyfrowego kamery, wówczas źródłem sygnału byłby radar położenia pojazdu lub zatopiona w podjeździe pętla indukcyjna. Wybór metody wyzwalania odczytu tablicy rejestracyjnej powinien zapewniać wysoką niezawodność funkcjonowania przejazdu do/z garażu podziemnego,
u) funkcjonalność kamery powinna zapewnić obsługę tzw. białej listy numerów rejestracyjnych. Lista będzie zawierała rekordy numerów rejestracyjnych wraz z przypisanymi do nich kodami kart (cardId),
v) kamera powinna umożliwiać przypisanie wielu numerom rejestracyjnym tego samego numeru cardId. Zapewnia to obsługę sytuacji, gdy jeden właściciel posiada kilka pojazdów, z których korzysta wymiennie,
w) w momencie rozpoznania tablicy rejestracyjnej pojazdu kamera powinna wysłać odpowiadający jej kod karty do kontrolera Systemu SKD. Kontroler Systemu SKD, zależnie od uprawnień właściciela pojazdu, przyzna mu prawa dostępowe do przejazdu lub odmówi dostępu,
x) kamera powinna umożliwiać import białej listy numerów rejestracyjnych z pliku,
y) kamera powinna być wyposażona w interfejs API, umożliwiający realizację funkcjonalności automatycznego przesyłania do kamery rekordów białej listy z bazy danych Systemu SKD (integracja). Wprowadzanie numerów rejestracyjnych właściciela pojazdu odbywa się w Systemie SKD, po czym następuje automatyczne rozesłanie danych do kamer ANPR,
z) kamera powinna być przystosowana do pracy w warunkach temperaturowych zewnętrznych w szerokim zakresie wilgotności powietrza, wymagana jest klasa szczelności IP67, klasa wytrzymałości IK10, z wbudowaną grzałką wewnętrzną,

aa) kamera powinna pracować w warunkach oświetlenia dziennego oraz nocnego, z wykorzystaniem promiennika podczerwieni, obiektyw kamery powinien zapewnić poprawny odczyt numeru rejestracyjnego dla zakresu od 3 do 20m,
bb) wymagana rozdzielczość minimalna to 4 MPixele, zapewniająca poprawną identyfikację pojazdu oraz wyraźny obraz na nagraniu,
cc) zasilanie kamery 12VDC lub PoE, powinno zapewniać nieprzerwaną pracę kamery przy braku zasilania sieciowego 230V przez minimum 4h.

VI. Wymagane cechy urządzeń blokujących

1) Bramka obrotowa wyposażona w mechanizm z systemem umożliwiającym udrożnienie przejścia, czyli takie ustawienie ramion, które pozwala na swobodne przejście. Może to nastąpić po otrzymaniu sygnału z centrali ppoż., pilota lub przycisku zbiciowo-ewakuacyjnego), powrót do trybu normalnego następuje automatycznie.
2) Dostęp do układu mechaniczno-elektrycznego zabezpieczony przed dostępem osób nieupoważnionych przez zastosowanie zamków na kluczyki.
3) Zintegrowany układ mechaniczno-elektrycznego, nie wymaga dodatkowych modułów, przekaźników, układów sterujących co znacznie zwiększa jego niezawodność.
4) Przygotowane miejsca do montażu czytników zbliżeniowych wewnątrz urządzenia zabezpieczone przed zakłóceniami.
5) Piktogram określający stan otwarcia/zamknięcia bramki (zielona strzałka/czerwony krzyżyk).
6) Przepustowość – 15-20 osób/min.

VII. Charakterystyka techniczna urządzeń blokujących

1) Pełna programowalność sygnałów sterujących zgodnie z wymaganiami klienta.
2) Konfigurowalne sygnały zwrotne, osobne dla każdego kierunku ruchu.
3) wyjście alarmowe informujące o próbie forsowania przejścia (możliwość podłączenia np. kamery).
4) Wyjście serwisowe sygnalizujące prawidłową pracę urządzenia lub awarię (np. zanik zasilania, przejście na zasilanie awaryjne itp.).
5) Wejście kasujące impulsy otwarcia – natychmiastowa blokada impulsów otwarcia (np. konfiguracja z detektorem metali).
6) Moduł zasilania awaryjnego (opcja dodatkowa) zapewniający ciągłą pracę – eliminujący zbędne straty przy przetwarzaniu AC/DC/AC (jak w UPS-ie) zamontowany bezpośrednio w urządzeniu.
7) Zabezpieczenie przed uszkodzeniem mechanicznym – sprzęgło cierne (przy dużym naporze na rotor znacznie ograniczona możliwość uszkodzenia mechanizmu).
8) Odblokowany ruch w obydwu kierunkach przypadku braku zasilania elektrycznego.
9) Sterowanie bezpotencjałowe lub potencjałowe 12÷24V.
10) Możliwość odblokowania przejścia sygnałem bezpotencjałowym z systemu SSP, przycisku ewakuacyjnego.
11) Wykonanie: stal nierdzewna.

VIII. Współpraca Systemu SKD z dźwigami osobowymi

1) Na terenie obiektu znajdują się dwie analogowe windy polskiej produkcji PUHP Pilawa, które obsługują budynek przy ul. Jasnej 6. Wymagana jest integracja obu wind z Systemem SKD w taki sposób, aby w Systemie SKD możliwe było nadanie poszczególnym pracownikom uprawnień do wjazdu tymi windami na wskazane piętra.
2) Wymogi integracji:
   a) w kabinach obu wind mają być zainstalowane czytniki Systemu SKD,
   b) w maszynowni wind, bądź pomieszczeniu przyległym, zostaną zainstalowane kontrolery SKD w wersji obsługującej integrację z windą. Kontrolery, wyposażone w moduły rozszerzeń wyjść, zostaną podłączone do szafy sterowniczej wind, przez uprawnionego instalatora z ramienia firmy mającej obsługę techniczną windy,
   c) dostęp do wybranego piętra będzie polegał na użyciu karty użytkownika na czytniku windowym a następnie, w ciągu kilku sekund, wciśnięciu przycisku danego piętra. Jeżeli użytkownik będzie posiadał uprawnienia dostępowe do wybranego piętra, winda ruszy i zrealizuje zlecenie,
   d) uprawnienia osób do wybranych pięter nadawane będą grupowo lub indywidualnie w Systemie SKD przez operatora Systemu.

IX. Współpraca Systemu SKD z bramą segmentową i szlabanami

1) Wjazd/wyjazd z garażu podziemnego budynku B6 wyposażony jest:
   a) w 2 istniejące odrębne szlabany (firmy CAME) – osobny dla kierunku „wjazd” i osobny dla kierunku „wyjazd”,
   b) w 1 wspólną istniejącą bramę segmentową (firmy HORMANN) dla obu kierunków ruchu,
   c) w 2 odrębne kamery ANPR (dodane w ramach projektu) – osobną dla kierunku „wjazd” i osobną dla kierunku „wyjazd”,
   d) w 2 odrębne detektory obecności pojazdów (dodane w ramach projektu) – osobny dla kierunku „wjazd” i osobny dla kierunku „wyjazd”,
   e) w 2 istniejące czytniki identyfikatorów – osobny dla kierunku „wjazd” i osobny dla kierunku „wyjazd”,
   f) dedykowany wideodomofon/domofon z dwoma panelami rozmównymi – jeden przy szlabanach, drugi wewnątrz garażu przy bramie segmentowej.
2) Wymagane jest doposażenie, wewnętrznych sterowników: bramy i szlabanów, w wyjścia bezpotencjałowe do sygnalizacji stanu ich położenia (zamknięte/otwarte) dla potrzeb Systemu Kontroli Dostępu SKD (biurowego).
3) Zasada działania SKD na wjeździe do garażu przedstawia się następująco: Uprawniony pojazd podjeżdża w oznaczone miejsce przed szlabanem „wjazdowym”. Następuje wykrycie obecności pojazdu przez detektor oraz aktywacja odczytu i rozpoznania jego tablicy rejestracyjnej przez kamerę ANPR. W momencie odnalezienia odczytanego

numeru rejestracyjnego pojazdu na białej liście w pamięci kamery, kamera wysyła, odpowiadający tej tablicy kod karty (identyfikatora właściciela/użytkownika pojazdu) do kontrolera Systemu SKD. Kontroler Systemu SKD, zależnie od uprawnień właściciela/użytkownika pojazdu, wyzwala podniesienie ramienia szlabanu „wjazdowego" i otwarcie bramy segmentowej. W kierunku na „wyjazd" działanie analogiczne.

4) Dla rowerzystów, osób bez wpisanego numeru tablicy rejestracyjnej pojazdu do Systemu SKD lub właścicieli/użytkowników uprawnionych pojazdów w sytuacjach, gdy odczyt i rozpoznanie tablicy rejestracyjnej nie jest możliwe, przewidziano do wykorzystania czytniki identyfikatorów zbliżeniowych (kart) lub obsługę wjazdu/wyjazdu przez służby ochrony wewnętrznej po kontakcie przez wideodomofony/domofony.
5) Obwody wykonawcze systemu wideodomofonowego/domofonowego muszą być podłączone do kontrolera SKD zespołu bramy segmentowej i szlabanów dla zachowania jednolitości sterowania oraz rejestracji faktu użycia wideodomofonu/ domofonu do otwarcia bramy i szlabanów.

X. Opis serwera Systemu SKD i terminali Systemu SKD

1) Oprogramowanie serwera Systemu SKD powinno być zbudowane w oparciu o relacyjną bazę danych Microsoft SQL Server 2022 (64 bity) wykorzystujące jej wersję płatną - Standard lub Enterprise Edition®.
2) Oprogramowanie zarządzające Systemu SKD powinno pracować na komputerach z systemami operacyjnymi: co najmniej Windows 10 Pro lub Windows 11, natomiast serwer Systemu SKD powinien pracować na komputerze z systemem operacyjnym co najmniej Windows Serwer 2022 (64 bity). Oprogramowanie Systemu SKD powinno wspierać pracę zarówno na maszynie fizycznej, jak i wirtualnej.
3) Architektura oprogramowania Systemu SKD winna być oparta o model klient - serwer:
   a) serwer główny (centralna baza danych) i serwis utrzymujący komunikację z kontrolerami SKD,
   b) stacje klienckie (terminale) - od 2 do 100 stanowisk operatorskich w różnych lokalizacjach, w tym stacja obsługi dla osób odwiedzających (interesantów) oraz stacja zarządzania kluczami.
4) Ze względu na planowane integracje serwer Systemu SKD powinien gwarantować wysoką dostępność świadczonych usług.
5) Maszyna fizyczna serwera powinna pracować w klimatyzowanej serwerowni, wyposażonej w gwarantowane źródło zasilania.
6) Baza danych powinna się znajdować na macierzy dyskowej, dane powinny być automatycznie backupowane.
7) System SKD powinien posiadać własną wydzieloną podsieć, własne routery oraz przełączniki sieciowe, nie podłączone bezpośrednio do pozostałej infrastruktury obiektu oraz sieci publicznej.

XI. Integracja Systemu SKD z systemem elektronicznej listy obecności

1) Oferowany System SKD powinien zapewniać funkcjonalność eksportu zarejestrowanych w nim zdarzeń, z wybranych przejść kontrolowanych, do pliku tekstowego *.csv w formacie określonym i wymaganym przez system elektronicznej listy obecności.

2) Eksport winien być wykonywany w trybach: automatycznym (z ustalonymi kryteriami czasowymi wykonania zadania) i „ręcznym" na żądanie operatora, z wykorzystaniem dedykowanego serwisu przeznaczonego do wykonywania tego zadania. Kryteria czasowe wykonywania zadania, miejsce zapisu pliku wynikowego (pliku eksportu *.csv), nazwa pliku itp. winny być definiowane w parametrach zadania eksportu, poprzez dedykowany interfejs GUI operatora.
3) Mechanizm eksportu powinien charakteryzować się następującymi cechami:
   a) zdarzenia zarejestrowane w Systemie SKD, pochodzące spoza grupy wybranych przejść winny być pomijane przy eksporcie do pliku *.csv,
   b) zdarzenia zarejestrowane w Systemie SKD, nie posiadające przypisanego im w słowniku Systemu SKD, kodu wymaganego przez system elektronicznej listy obecności, winny być pomijane przy eksporcie do pliku *.csv,
   c) zdarzenia zarejestrowane w Systemie SKD, przez osoby zarejestrowane w bazie danych w Systemie SKD, ale nie posiadających przypisanych im numerów identyfikacyjnych (unikalnych) obowiązujących dla tych osób w systemie elektronicznej listy obecności, winny być pomijane przy eksporcie do pliku *.csv.

XII. Integracja Systemu SKD z zewnętrznym systemem RCP

1) Oferowany System SKD powinien zapewniać funkcjonalność dwukierunkowej integracji baz danych: Systemu SKD i zewnętrznego systemu RCP w opisanym niżej zakresie.
2) W przedstawionym opisie przyjęto, że oba systemy korzystają z baz danych Microsoft SQL.
3) Przez dwukierunkową integrację baz danych należy rozumieć funkcje:
   a) synchronizacji danych osobowych, pracowników zdefiniowanych w bazie danych zewnętrznego systemu RCP z bazą danych SKD. Przy tym za „źródłową" bazę danych należy przyjąć bazę danych zewnętrznego systemu RCP. W bazie „źródłowej" każdy odnotowany pracownik winien posiadać unikalny numer identyfikacyjny, który będzie „kluczem identyfikacyjnym" dla Systemu SKD i będzie przepisywany do bazy danych SKD do odpowiedniego pola danych identyfikacyjnych w SKD,
   b) udostępniania zewnętrznemu systemowi RCP, zarejestrowanych w bazie danych Systemu SKD zdarzeń, z wybranych przejść kontrolowanych, na ustalonych w Systemie SKD zasadach.
4) Dla celów opisywanej tu integracji dwukierunkowej dopuszczone jest wykorzystywanie dedykowanych widoków MSSQL lub serwisów Web API. Przy czym formaty: oczekiwanego przez System SKD, widoku z danymi osobowymi udostępnianymi przez zewnętrzny system RCP oraz widoku ze zdarzeniami RCP udostępnianego przez System SKD na potrzeby zewnętrznego systemu RCP, określa System SKD.
5) W przypadku wykorzystania serwisu Web API, metody wykorzystane do tej integracji określa System SKD.
6) Synchronizacja danych osobowych winna odbywać się w trybach: automatycznym (z ustalonymi kryteriami czasowymi wykonania zadania) i „ręcznym" na żądanie operatora, z wykorzystaniem dedykowanego serwisu przeznaczonego do wykonywania tego zadania. Kryteria czasowe wykonywania zadania i inne parametry do połączenia się z bazą danych zewnętrznego systemu RCP i odczytywania danych osobowych, pracowników tam

zarejestrowanych, za pomocą dedykowanego widoku SQL winny być definiowane w parametrach zadania eksportu, poprzez dedykowany interfejs GUI operatora.

7) Synchronizacja danych osobowych pracowników w obu bazach w ramach opisywanej integracji winna zapewnić ich „współbieżność", czyli dodanie danych osobowych nowego pracownika do zewnętrznego systemu RCP winno skutkować odwzorowaniem tych danych w Systemie SKD. Podobnie, usunięcie danych pracownika z zewnętrznego systemu RCP lub ich modyfikacja, powinna być automatycznie odwzorowywana w Systemie SKD.
8) Mechanizm udostępniania danych o zdarzeniach RCP winien charakteryzować się następującymi cechami:
   a) zdarzenia zarejestrowane w Systemie SKD, pochodzące spoza grupy wybranych przejść winny być pomijane przy prezentacji w widoku SQL dla potrzeb zewnętrznego systemu RCP,
   b) zdarzenia zarejestrowane w Systemie SKD, nie posiadające przypisanego im w słowniku Systemu SKD, kodu wymaganego przez zewnętrzny system RCP, winny być pomijane przy prezentacji w widoku SQL dla potrzeb zewnętrznego systemu RCP,
   c) zdarzenia zarejestrowane w Systemie SKD, przez osoby zarejestrowane w bazie danych w Systemie SKD, ale nie posiadających przypisanych im numerów identyfikacyjnych (unikalnych) obowiązujących dla tych osób w zewnętrznym systemie RCP, winny być pomijane przy prezentacji w widoku SQL dla potrzeb zewnętrznego systemu RCP,
   d) widok SQL ze zdarzeniami zarejestrowanymi w Systemie SKD, prezentowanymi dla potrzeb zewnętrznego systemu RCP, winien być automatycznie ograniczany tylko do rekordów (ze zdarzeniami), które nie zostały odczytane przez zewnętrzny System RCP.

XIII. Integracja Systemu SKD z systemem depozytorów kluczy

1) Oferowany System SKD powinien zapewniać integrację z systemem depozytorów kluczy (gdzie baza Systemu SKD jest bazą nadrzędną).
2) Integracja (między bazami: baza Systemu SKD – baza depozytorów kluczy) ma zapewnić co najmniej:
   a) automatyczny i ręczny (na żądanie) eksport danych personalnych pracownika z bazy SKD do bazy depozytora/ów (synchronizacja danych osobowych w bazach),
   b) blokowaniu w trybie ON LINE zdolności pobrania klucza/-y przez pracownika bez uprzedniego odnotowania przez SKD wejścia pracownika do obszaru kontrolowanego (np. na teren Sądu),
   c) blokowaniu w trybie ON LINE możliwości wyjścia pracownika przez przejście kontrolowane SKD bez wcześniejszego zdania klucza do depozytora, uprzednio z niego pobranego,
   d) blokowaniu w trybie ON LINE możliwości wyjścia ostatniego pracownika z grupy uprawnionych do danego klucza bez uprzedniego zdania tego klucza do depozytora,
   e) obsługi wielu depozytorów w różnych lokalizacjach (budynkach) z uwzględnieniem powyższych opcji.

XIV. Integracja Systemu SKD z systemem sygnalizacji włamania i napadu

Do wskazanych przez Zamawiającego pomieszczeń technicznych należy wdrożyć funkcjonalność czasowego blokowania i odblokowania wybranych linii alarmowych systemu sygnalizacji włamania i napadu poprzez dwukrotne użycie karty kontroli dostępu z odpowiednimi uprawnieniami.

XV. Integracja Systemu SKD z systemem sygnalizacji alarmu pożarowego

Funkcje Centrali Kontroli Dostępu podczas akcji pożarowej i ewakuacji przejmuje Centrala Systemu Sygnalizacji Pożarowej (SSP). W czasie akcji pożarowej i ewakuacji otwieranie drzwi następuje na podstawie algorytmu zawartego w Centrali Systemu Sygnalizacji Pożarowej, która działa bezpośrednio na przejście kontrolowane za pomocą certyfikowanego modułu wykonawczego, galwanicznie rozwierając zasilanie drzwi ewakuacyjnych.
System SSP działa jako system nadrzędny w stosunku do SKD i to właśnie system SSP decyduje o otwarciu drzwi bezpośrednio oddziaływując na element blokujący (przerwanie obwodu zasilającego element blokujący) oraz zwolnieniu tripodów i bramek uchylnych poprzez odcięcie zasilania.

XVI. System wizualizacji.

1) Oferowany system wizualizacji SKD powinien zapewniać możliwość wizualizacji i integracji różnych rodzajów systemów bezpieczeństwa (SSWiN, SKD, CCTV, SSP), w tym systemów sygnalizacji pożaru obecnie użytkowanych w budynkach NSA.
2) Należy wdrożyć system wizualizacji Systemu SKD spełniający następujące wymagania minimalne:
   a) obsługa na minimum 5 stanowiskach komputerowych,
   b) obsługa przez minimum 12 operatorów o zróżnicowanych uprawnieniach,
   c) obsługa przez aplikację kliencką,
   d) bieżąca aktualizacja stanów przejść za pomocą elementów aktywnych – drzwi oraz czytników,
   e) możliwość zdalnego odblokowania/blokady wybranych przejść przez operatora z poziomu mapy obiektu,
   f) sygnalizacja stanów alarmowych i ostrzeżeń, potwierdzanie podjętych przez operatora akcji,
   g) graficzna prezentacja obiektu, oparta na podkładach budowlanych (technologia 2D lub 3D),
   h) prezentacja aktywnych obrazów graficznych w aplikacji klienckiej,
   i) wbudowany interfejs do modyfikacji graficznej prezentacji obiektu, w tym dodawania nowych elementów aktywnych z dostępnej biblioteki lub modyfikacja istniejących.

XVII. Uwagi końcowe

1) Całość prac powinna być wykonana według obowiązujących przepisów, norm branżowych i wiedzy technicznej.
2) Przed uruchomieniem instalacji Systemu należy wykonać badania polegające na sprawdzeniu:

a) poprawności połączeń,
b) umocowania połączeń,
c) właściwej numeracji elementów,
d) adresów i oznakowania elementów,
e) właściwego oprogramowania Systemu.

3) Uruchomienie Systemu należy wykonać zgodnie z instrukcją instalacji Systemu dostarczoną przez Wykonawcę.
4) Zamawiający uwzględni zmiany projektu w zakresie ilości kontrolerów dla 103 przejść. Zaproponowane kontrolery mogą obsługiwać nie więcej niż 4 przejścia. Wszelkie planowane zmiany i odstępstwa od projektu Systemu SKD należy uzgodnić z Zamawiającym.
5) Po zakończeniu prac Wykonawca zobowiązany jest przekazać dokumentację powykonawczą, zawierającą:
   a) zaktualizowaną część opisową i rysunkową,
   b) protokół sprawdzenia poprawności działania Systemu (sprawdzeniu podlega wszystkich elementów Systemu),
   c) protokół współdziałania Systemu z innymi systemami, kompletne instrukcje obsługi i konserwacji dla wszystkich urządzeń oraz instrukcję obsługi Systemu.
6) Wszystkie instalacje przechodzące przez przegrody przeciwpożarowe muszą być uszczelnione masą o odporności ogniowej równej odporności przegrody. Prace te należy wykonywać, gdy sama instalacja jest już ukończona. Uszczelnienie należy wykonać zgodnie z polskimi normami, stosownymi przepisami i instrukcjami.
7) Wymaga się przeprowadzanie okresowych przeglądów Systemu zgodnie z zaleceniami instrukcji obsługi Systemu, jednak nie rzadziej niż raz w roku.
8) Przeglądy okresowe powinny być wykonywane przez wyspecjalizowany personel posiadający odpowiednie uprawnienia i wiedzę techniczną.
9) Jeżeli w wyniku okresowych przeglądów stwierdzona zostanie konieczność naprawy lub konfiguracji Systemu, Wykonawca przeprowadzi niezbędne prace w ramach gwarancji.
10) Dostarczone oprogramowanie powinno być zarejestrowane na Zamawiającego.