

Opis przedmiotu zamówienia

I. Ogólny opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostawa wraz z instalacją Systemu Bezprzewodowej Kontroli Dostępu w budynku wraz integracją z istniejącym SSWiN oraz CCTV.

Do chwili obecnej dostęp do poszczególnych pomieszczeń biura jest możliwy za pomocą tradycyjnych kluczy i zamków patentowych. Na parterze budynku zainstalowany jest system kontroli dostępu w drzwiach: wejściowych głównych, wiatrołapu, wejściowych od strony garaży.

W celu zwiększenia bezpieczeństwa projektuje się system bezprzewodowej kontroli dostępu, który obejmie:

- drzwi wejściowe – piwnica;
- wszystkie pomieszczenia biurowe;
- dostęp do poszczególnych skrzydeł budynku (dwa na każde piętro);
- drzwi do pokoi gościnnych (5 piętro)

oraz przewodowy dostęp:

- drzwi wejściowe do budynku (drzwi główne oraz od strony garaży)
- drzwi wejściowe – wiatrołap;

Autoryzacja dostępu użytkowników będzie realizowana za pomocą posiadanych w całej organizacji kart kryptograficznych, które zapewniają wysoki poziom bezpieczeństwa i zgodność z wewnętrznymi standardami. Używane karty obsługują interfejs stykowy i bezstykowy. Do zarządzania ich cyklem życia stosowany w organizacji jest system HID ActivID Credential Management System. Współpracując z oprogramowaniem pośredniczącym HID ActivClient, wspierają standardy CryptoAPI i PKCS#11 w środowiskach Windows 10 i 11 (32/64-bit). Karty oferują wsparcie dla algorytmów: AES-128, Triple DES, RSA 1024/2048, ECC, przechowują minimum cztery certyfikaty, umożliwiają wdrażanie polityki haseł oraz spełniają wymagania normy ISO/IEC 7816-3:2006/AMD1:2025 (interfejs fizyczny), są zgodne ze specyfikacją GlobalPlatform Card Specification v2.2.1 lub wyższą, zgodną wstecznie i platformą JavaCard 3.0.4 lub wyższą.

Każdy uprawniony użytkownik będzie korzystał z dedykowanej karty do uwierzytelniania i otwierania przejść zgodnie z nadanymi uprawnieniami.

Dla gości oraz użytkowników tymczasowych dostęp będzie generowany poprzez aplikację mobilną, umożliwiającą korzystanie z technologii komunikacji bezprzewodowej krótkiego zasięgu, w tym: standardu NFC (Near Field Communication); energooszczędnej komunikacji bezprzewodowej w paśmie 2,4 GHz, zgodnej z technologią Bluetooth Low Energy (BLE) lub równoważną w celu autoryzacji na kompatybilnych czytnikach. Mobilne poświadczenia będą przydzielane indywidualnie i zarządzane z poziomu wdrożonego systemu kontroli dostępu.

1. Cel zamówienia:

- a. Zwiększenie bezpieczeństwa dostępu do budynku oraz pomieszczeń biura ;
- b. Poprawa organizacji i efektywności;
- c. Możliwość analizy ruchu oraz raportowania danych.

2. Zakres przedmiotu zamówienia:

- a. Przedmiotem zamówienia jest dostawa oraz montaż:
 - Okuć elektronicznych z modułem kontroli dostępu z czytnikiem kart (drzwi wewnętrzne);
 - Czytników kontroli dostępu z dwuskładnikowym uwierzytelnieniem (karta + PIN);

- Elektrozaczepeków do drzwi wejściowych;
 - Węzły komunikacyjne (hub) umożliwiające integrację bezprzewodową czytników;
 - Kamer kopułowych (1 wewnętrzna, 2 do rozpoznawania tablic rejestracyjnych samochodów);
 - Depozytora kluczy - Klucze przechowywane będą w kieszeniach z mechaniczną blokadą wyjęcia. Pobranie klucza możliwe będzie wyłącznie przez uprawnionych użytkowników. Użytkownicy systemu będą identyfikowani za pośrednictwem karty zbliżeniowej. Uprawnienia określają, które klucze i kiedy mogą być pobrane przez konkretnych użytkowników systemu – minimum 8 szt.;
 - Oprogramowanie zarządzające umożliwiające zarządzanie dostępem oraz dające możliwość integracji z innymi systemami zewnętrznymi (np. system alarmowy, monitoring, automatyka bramy wjazdowej);
 - Mobilne licencje dostępowe – umożliwiające pełną integrację z wdrożonym systemem kontroli dostępu (min. 10 szt.)
- b. Realizacja zamówienia odbędzie się na zasadach i warunkach ujętych we wzorze umowy, stanowiącym załącznik nr 9 do SWZ.

3. Opis funkcjonalności:

- a. Podstawowe funkcje systemu:
- Autoryzacja i zdalne zarządzanie dostępem;
 - Monitorowanie i rejestrowanie zdarzeń;
 - Integracja z innymi systemami różnych producentów (systemy alarmowe, CCTV);
 - Bezpieczeństwo i niezawodność (szyfrowanie komunikacji, możliwość pracy online, funkcja anti-passback);
 - Integracja z Active Directory.

II. Zakres prac i usługi

1. Dostawa, wymagania techniczne i funkcjonalne:

Urządzenia muszą być fabrycznie nowe i wyprodukowane nie wcześniej niż 12 miesięcy przed datą dostarczenia.

Wszystkie oferowane urządzenia muszą być w momencie składania oferty zgodne z obowiązującymi przepisami dotyczącymi wprowadzenia do obrotu, w szczególności zgodnie z art. 10 ust. 11 dyrektywy 2014/53/UE.

Urządzenia nie mogą być wycofane z obrotu przez producenta i muszą być dopuszczone do użytkowania na rynku Unii Europejskiej.

2. Montaż urządzeń:

Pomieszczenia, w których powinny zostać zamontowane okucia bezprzewodowe powinny zostać skomunikowane bezprzewodowo z całością systemu. W związku z tym należy rozproszyc odbiorniki sygnału w taki sposób, aby zapewnić komunikację ze wszystkimi okuciami bezprzewodowymi w budynku biura.

Należy dostarczyć taką ilość odbiorników sygnału, aby jednocześnie wszystkie okucia bezprzewodowe były w trybie online.

Przejścia, w których zostaną zamontowane czytniki przewodowe muszą zostać skomunikowane z całością systemu i posiadać zabezpieczenia w postaci elektrozaczepek oraz samozamykacza.

3. Dokumentacja:

Wykonawca zobowiązany jest dostarczyć dokumentację powykonawczą zawierającą:

- a. szczegółowy opis wykonanych prac,
- b. schematy instalacji i połączeń,
- c. wyniki pomiarów okablowania strukturalnego przeprowadzone certyfikowanym testerem poziomu V lub wyższym, zgodnym z wymaganiami norm ISO/IEC 11801, lub równoważne oraz EC 61935-1:2019 , lub równoważne, dla odpowiedniej klasy okablowania (np. klasa E/EA/Kategoria 6/6A). Raporty pomiarowe w formie elektronicznej, zawierające szczegółowe dane (np. NEXT, FEXT, Return Loss, ACR-F, TCL, ELTCTL), muszą zostać dołączone do dokumentacji powykonawczej. ,

4. Szkolenia i wsparcie:

Wykonawca przeprowadzi szkolenie z zakresu obsługi i administracji wdrożonego systemu kontroli dostępu dla minimum 4 osób.

5. Wymagania dotyczące oprogramowania:

- a. Ogólne wymagania systemowe:
 - Otwarta architektura (obsługa kontrolerów różnych producentów – min. 4);
 - Integracja z systemami VMS;
 - Zaimplementowane funkcje systemowe: Anti-passback, Classroom Mode, wymóg dwóch kart dla wejścia, aktywacja harmonogramu po pierwszym wejściu, limit wejść;
 - Obsługa zamków bezprzewodowych minimum dwóch różnych producentów;
 - Wsparcie dla czytników OSDP;
 - Interfejs użytkownika w języku polskim, dostępny przez przeglądarkę;
 - Działanie przynajmniej na dwóch systemach operacyjnych (Microsoft Windows oraz jednej dystrybucji Linux);
 - Możliwość wirtualizacji systemu;
 - Aplikacja mobilna dla Android a także iOS;
- b. Funkcjonalność dostępu i identyfikacji:
 - Obsługa różnych metod uwierzytelniania: karty RFID 13,56 MHz; PIN; kod QR; uwierzytelnianie mobilne; tablice rejestracyjne pojazdów;
 - Zarządzanie windami;
 - Integracja z systemami SSWiN (uzbrajanie/rozbrajanie stref z poziomu czytnika).
- c. Monitorowanie i raportowanie:
 - Możliwość monitorowania zdarzeń i alertów;
 - Podgląd wideo w momencie uzyskania dostępu (integracja z CCTV);
 - Obsługa map obiektów (wizualizacja zdarzeń i alarmów);
 - Raporty dostępu (lista użytkowników);
- d. Integracja i automatyzacja:
 - Bezpłatne API REST do komunikacji z innymi systemami;
 - Import użytkowników z Active Directory oraz plików CSV;
 - Automatyzacja działań (aplety IFTTT);
 - Obsługa szlabanów parkingowych.
- e. Bezpieczeństwo i baza danych:

- Możliwość automatycznego tworzenia kopii zapasowych bazy danych;
- Możliwość korzystać z bezpłatnej, komercyjnej bazy danych typu SQL (np. PostgreSQL).
- Implementacja logicznej segmentacji bazy danych, umożliwiająca dostęp do określonych obiektów i stref.

6. Prawo opcji:

Zamawiający przewiduje możliwość skorzystania z Prawa Opcji. Zakres i warunki wymagane określa szczegółowo pkt. 3.2 SWZ.

7. Bezpieczeństwo i certyfikaty:

a. Szyfrowanie i bezpieczeństwo transmisji:

- System kontroli dostępu musi wykorzystywać zaawansowane mechanizmy kryptograficzne w celu zabezpieczenia transmisji danych pomiędzy urządzeniami wchodzącymi w skład systemu (klamka, czytnik, kontroler, hub, serwer zarządzania, urządzenia mobilne);
- Szyfrowana komunikacja RS-485 między czytnikami a kontrolerami dostępu;
- VPN / IPsec dla połączeń zdalnych do systemu, eliminacja ruchu nieszyfrowanego;
- Wymagane standardy szyfrowania AES-256, TLS 1.3
- Dla uwierzytelniania urządzeń bezprzewodowych – Elliptic Curve Cryptography (ECC);
- Ochrona przed przechwyceniem i podsłuchem transmisji;

b. Certyfikaty i normy techniczne, które musi spełniać system:

- Normy dotyczące bezpieczeństwa IT - PN-EN ISO/IEC 27001:2023-08, lub równoważne ;
- urządzenia oferowane w ramach dostawy systemu kontroli dostępu muszą spełniać wymagania określone w następujących normach (lub równoważnych), co musi być potwierdzone odpowiednim certyfikatem:
 - ISO/IEC 15408-1:2022 (Common Criteria), poziom EAL4+ lub wyższy – dla urządzeń kontroli dostępu (KD), potwierdzone certyfikatem CC EAL4+ lub równoważnym;
 - Spełniać standardy bezpieczeństwa FIPS PUB 140-2 lub FIPS PUB 140-3 – dla modułów kryptograficznych, potwierdzone stosownym certyfikatem FIPS;
 - Dyrektywą 2014/53/UE (RED) oraz oznakowanie CE – dla urządzeń bezprzewodowych, potwierdzone certyfikatem zgodności (np. deklaracją zgodności UE lub innym dokumentem wystawionym przez producenta lub jednostkę notyfikowaną).

8. Warunki gwarancji i rękojmi:

- a. Zamawiający wymaga, aby Wykonawca udzielił min. 24 miesięcznej gwarancji i rękojmi na przedmiot umowy, licząc od dnia wykonania zamówienia, potwierdzonego sporządzeniem bezusterkowego protokołu odbioru.
- b. Zamawiający wymaga, aby Wykonawca wykonał w każdym roku obowiązywania gwarancji 1 przegląd serwisowy, obejmującego:

- Prawidłowości działania systemu;
 - Kontrolę baterii w okuciach i w razie konieczności ich wymianę (koszt baterii ponosi Zamawiający);
 - Kontrolę działania połączeń bezprzewodowych oraz kablowych on-line.
- c. Szczegółowe warunki gwarancji i rękojmi opisane są szczegółowo w pkt.: 4.3, 4.4 SWZ.

9. Wymagania dotyczące interoperacyjności:

- a. Możliwość współpracy urządzeń różnych producentów w ramach otwartych protokołów;
- b. Otwartość systemu i możliwość rozbudowy umożliwiająca dodawanie nowych funkcji, urządzeń oraz integracji z innymi systemami (systemy alarmowe, CCTV, BMS);
- c. Możliwość rozbudowy bez konieczności wymiany całego systemu.

III. Załączniki:

1. Załącznik A – Wymagania funkcjonalne;
2. Załącznik B – Zakres prac;
3. Załącznik C – Plan budynku ze schematem rozmieszczenia urządzeń;
4. Załącznik D – Wymagania funkcjonalno-techniczne.