

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest wykonanie dostawy i montażu systemu kontroli dostępu oraz dostawa i montaż depozytora do kluczy w budynku OUD W Bydgoszczy z siedzibą w Trzszynie Generalnej Dyrekcji Dróg Krajowych i Autostrad Oddział w Bydgoszczy.

1. Założenia ogólne

Celem instalacji systemu jest umożliwienie kontroli dostępu do pomieszczeń w budynku Obwodu Utrzymania Dróg w Bydgoszczy z siedzibą w Trzszynie, przy wykorzystaniu dedykowanych kart.

Montaż depozytora do kluczy w ilości min. 16 sztuk, nie więcej jak 20 sztuk, funkcjonalnie połączonego w jeden system z kontrolą dostępu, ma ułatwić zarządzanie dostępem do pomieszczeń pracowniczych OUD Bydgoszcz i uniemożliwić dostęp osobom nieupoważnionym.

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

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).
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.

2. Wymagania i funkcjonalności systemu

2.1 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).
- 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), Aplikacje interfejsu użytkownika muszą prezentować zunifikowany interfejs bezpieczeństwa do zarządzania, konfigurowania, monitorowania i raportowania systemów ACS oraz powiązanych urządzeń brzegowych.
- Aplikacja musi zapewniać m.in.:

- a) Obsługę i konfigurację systemów takich jak ACS.
 - b) Monitorowanie zdarzeń bieżących i odtwarzanie zarchiwizowanych materiałów wizyjnych.
 - c) Zarządzanie alarmami.
 - d) Raportowanie, w tym tworzenie niestandardowych szablonów raportów i raportów o incydentach.
- Obsługę minimum 30 użytkowników i 10 przejść.
 - 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 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, xls, 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)
 - Bezterminowe licencje na wszystkie aplikacje i moduły oprogramowania wchodzące w skład systemu.

3. 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. 10 przejść kontrolowanych za pośrednictwem modułów rozszerzających.

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
- ochronę złącza rozszerzającego kontrolera przez szyfrowanie w AES (seria 3 SIO),
- wsparcie dla OpenSSL,
- w przypadku zastosowania dodatkowych elementów takich jak np. moduły rozszerzeń mogą one być rozmieszczone w bezpośredniej bliskości przejść kontrolowanych.

4. Czytnik kart

Czytniki zbliżeniowe zainstalowane do odczytu kart, muszą obsługiwać protokół OSDP. Rozmiar czytników powinien być standardowy 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: różnica temperatur nie mniejsza niż 20°C
- klasa środowiskowa IP44
- obsługa technologii MIFARE Classic, MIFARE DESFire EV1 i iCLASS
- zgodność z normami ISO14443A (MIFARE) CSN, ISO14443B CSN, ISO15693 CSN

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

- 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.

5. Przejścia

Wszystkie przejścia jednostronne muszą zostać zamontowane w taki sposób, aby wejście możliwe dzięki użyciu karty z odpowiednimi uprawnieniami lub klucza dopasowanego do istniejącej wkładki, natomiast wyjście umożliwiać będzie klamka lub przycisk zwalniający blokadę.

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 otwarcie drzwi bez autoryzacji lub klucza.

5.1 Elektrozaczepek

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

Minimalne wymagania dla elektrozaczepeków montowanych w pozostałych przejściach:

- a) elektrozaczepek rewersyjny (NO) z czujnikiem i monitoringiem,
- b) możliwość regulacji,
- c) może być stosowany do drzwi lewych i prawych.

5.2 Zwora elektromagnetyczna

Montowane elementy tego typu powinny spełniać poniższe wymagania:

- a) montaż nawierzchniowy,
- b) możliwość zasilania prądem o napięciu 12 lub 24V.

6. Urządzenia sieciowe

Do obsługi komunikacji wszystkich urządzeń systemu kontroli dostępu z wykorzystaniem protokołu TCP/IP, Wykonawca dostarczy i zainstaluje dedykowane przełączniki sieciowe.

7. Dokumentacja powykonawcza

Po zakończeniu prac instalacyjnych i konfiguracyjnych systemu Wykonawca przekaze Zamawiającemu dokumentację powykonawczą zawierającą:

1. Plany poszczególnych budynków z naniesionymi elementami instalacji (czytniki, przyciski, zaczepty, 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.

Warunki udziału w postępowaniu:

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki dotyczące zdolności technicznych lub zawodowych – doświadczenie:
Wykonawca musi wykazać, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie należyce wykonał jedno lub dwa zamówienia (rozumiane jako jedną lub dwie odrębne umowy) polegające na montażu systemów kontroli dostępu, na łączną kwotę minimum 15 000,00 zł brutto.

Zamawiający zastrzega, że w przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia (np. konsorcja, spółki cywilne), potencjał podmiotów nie podlega sumowaniu, tj. co najmniej jeden z Wykonawców wspólnie ubiegających się o udzielenie zamówienia musi wykazać się indywidualnie wymaganym powyżej doświadczeniem.

2. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki dotyczące zdolności technicznych lub zawodowych – potencjał techniczny wykonawcy:
Wykonawca musi złożyć oświadczenie, wraz z dokumentem potwierdzającym, o posiadaniu uprawnień do wykonywania przedmiotu zamówienia,
3. Koncesję MSWiA na prowadzenie działalności w zakresie usług ochrony osób i mienia realizowanych w formie zabezpieczenia technicznego wynikającej z ustawy.
4. Posada niezbędną wiedzę i doświadczenie oraz dysponuje potencjałem technicznym i osobami zdolnymi do wykonania Zamówienia.
5. Posiada uprawnienia do wykonania określonej działalności, jeżeli przepisy prawa nakładają obowiązek ich posiadania.
6. Świadectwo kwalifikacyjne dozoru i eksploatacji urządzeń, instalacji i sieci min. 1 kV.
7. Polisę ubezpieczeniową od odpowiedzialności cywilnej w zakresie prowadzenia działalności na sumę gwarancyjną nie mniejszą niż 100 000 PLN.

Termin realizacji:

Przedmiot zamówienia obejmuje wykonanie realizacji w terminie do 4 tygodni od dnia podpisania umowy.

Termin płatności:

Wynagrodzenie będzie płatne na podstawie prawidłowo wystawionej i dostarczonej przez Wykonawcę faktury VAT, w terminie 14 dni kalendarzowych od daty jej otrzymania, na rachunek bankowy Wykonawcy wskazany na fakturze.

Kryteria wyboru i sposób oceny ofert:

Przy dokonywaniu wyboru najkorzystniejszej oferty Zamawiający stosować będzie następujące kryterium oceny ofert: Cena – 100%

Kryterium będzie rozpatrywane na podstawie ceny brutto za wykonanie przedmiotu zamówienia, podanej przez Wykonawcę w Formularzu ofertowym.

Zamawiający ofercie o najniższej cenie przyzna 100 punktów, a każdej następnej zostanie przyporządkowana liczba punktów proporcjonalnie mniejsza, według wzoru:

$$C = (C_{\min} / C_o) \times 100 \text{ pkt}$$

gdzie:

C_{\min} – najniższa cena brutto z ocenianych ofert (zł)

C_o – cena brutto określona w badanej ofercie (zł)

Za najkorzystniejszą zostanie uznana oferta, która otrzyma najwyższą liczbę punktów.