Załącznik nr 8 do „Zapytania ofertowego"

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem postępowania jest dostarczenie wszystkich niezbędnych urządzeń, wykonanie instalacji, konfiguracji systemu kontroli dostępu w 26 podstacjach NN MPK – Łódź. W podstacjach należy wykonać instalację systemu KD dla pojedynczego wejścia.

1. Lokalizacje podstacji NN

Lp.	Nr stacji	Nazwa	Adres stacji	Istniejący obecnie typ centrali alarmowej
1	**1**	**WĘGLOWA**	Węglowa	integra 64
2	**3**	**STOCKA**	Łódź ul. Stocka 15	integra32
3	**4**	**PRZECHODNIA**	Łódź ul. Przechodnia 30	integra32
4	**6**	**1-GO MAJA**	Łódź ul.1-go Maja 58	integra32
5	**7**	**PIOTRKOWSKA**	Łódź ul. Piotrkowska 77	integra32
6	**8**	**ZACHODNIA**	Łódź ul. Zachodnia 23	integra32
7	**9**	**WRÓBLEWSKIEGO**	Łódź ul. Władysława Króla 2	integra 64
8	**10**	**HELENÓWEK**	Łódź ul. Zgierska 252/254	integra32
9	**11**	**CHOCIANOWICE**	Łódź ul. Pabianicka 215	integra32
10	**17**	**WACŁAWA**	Łódź ul. Wacława 7	integra 64
11	**18**	**SMUGOWA**	Łódź ul. Smugowa 16	integra 64
12	**19**	**ZGIERSKA**	Łódź ul. Zgierska 184/186	integra32
13	**20**	**PIŁSUDSKIEGO**	Łódź ul. Piłsudskiego 145	integra 64
14	**26**	**REMBIELIŃSKIEGO**	Łódź ul. Rembielińskiego 29	integra32
15	**27**	**STARORUDZKA**	Łódź ul. Starorudzka 4/6	integra32
16	**29**	**KOPERNIK**	Łódź Al. Jana Pawła II 5	integra 64
17	**30**	**KĘS**	Łódź ul. Legionów 14	integra32
18	**31**	**ŚRÓDMIEŚCIE**	Łódź ul. Sienkiewicza 99	integra 64
19	**32**	**TELEFONICZNA**	Łódź ul. Telefoniczna 40	integra 64
20	**35**	**PAROWOZOWA**	Łódź ul. Parowozowa 5/7	integra 64
21	**36**	**ZAPOLSKA**	Łódź ul. Zapolskiej 11/13	integra 64
22	**37**	**HETMAŃSKA**	Łódź ul. Hetmańska	integra 64
23	**40**	**ŁĄKOWA**	Zgierz ul. Łąkowa dz.nr.296/22	integra128
24	**41**	**DUŻY SKRĘT**	Pabianice ul. Warszawska 148a-152	integra 64
25	**42**	**ŻEROMSKIEGO**	Pabianice ul. Żeromskiego 3	integra 64
26	**43**	**PRZYGRANICZNA**	Konstantynów Łódzki ul. Aleksandrowska 100	integra128

Zgodnie z założeniami system KD obejmuje instalację urządzeń oraz instalację kablową dla 1 przejścia kontroli dostępu - drzwi wejściowych zewnętrznych (realizujących ruch dwukierunkowy) w każdym budynku podstacji NN. Sterowanie drzwiami należy

zrealizować za pomocą zwory elektromagnetycznej o udźwigu 350 kg oraz czytnika zbliżeniowego kart Mifare Classic zainstalowanego od strony zewnętrznej drzwi. W obwód zasilania zwory należy wpiąć przycisk ewakuacyjny od strony wewnętrznej drzwi oraz stacyjkę od strony zewnętrznej. Funkcję jednostki centralnej pełni kontroler dostępu, który zbiera dane z czytnika wejściowego i po pozytywnym zweryfikowaniu karty zwalnia blokadę elektromagnetyczną oraz rozbraja system SSWiN umożliwiając wejście do budynku. Przy wyjściu z budynku należy użyć przycisku wyjścia. Zamawiający wymaga aby w systemie centralnym na mapie były prezentowane stany central alarmowych podstacji NN Uzbrojenie/Rozbrojenie/Alarm. Wykonawca zwizualizuje na mapie wszystkie podstacje NN w aplikacji Zamawiającego Veno-Is wraz z ich statusami on-line. Z poziomu aplikacji centralnej (Veno) musi być możliwość zdalnego uzbrojenia i rozbrojenia systemu SSWiN. W systemie musi być sygnalizacja użycia przycisku ewakuacyjnego oraz informacja o stanie drzwi z czujnika drzwi. Wszystkie podstację posiadają routery z dostępem do sieci Zamawiającego. Po stronie Wykonawcy jest wykonanie instalacji do routera i centrali alarmowej oraz dostarczenie niezbędnych modułów rozszerzeń oraz urządzeń umożliwiających podłączenie kontrolera do centrali alarmowej umożliwiających osiągniecie wymaganej funkcjonalności (zbieranie informacji o stanie centrali i uzbrojenie/rozbrojenie/alarm).

W przypadku awarii kontrolera można wejść do budynku poprzez zewnętrzną stacyjkę, a wyjść przy użyciu przycisku ewakuacyjnego.

Użycie przycisku ewakuacyjnego musi być zasygnalizowane w systemie centralnym Zamawiającego.

Kontroler powinien pracować w trybie klient-serwer. Komunikację z serwerem zrealizować poprzez router. Kontroler powinien obsługiwać minimum 20 000 kart oraz bufor o min 20 000 zdarzeń. Użycie karty lub przycisku ewakuacyjnego powinno zostać odnotowane i przesłane do systemu. System musi umożliwiać dodawanie i odbieranie uprawnień kart w czasie rzeczywistym na wszystkich obiektach. System musi rejestrować każde użycie karty, zarówno kart dozwolonych, jak i zabronionych.

Urządzenia powinny być oficjalnie dystrybuowanym seryjnym produktem przeznaczonym do pracy w ciągłej (24/7).

Za pośrednictwem obecnie użytkowanych kart pracowniczych Mifare Classic Plus X pracownicy Zamawiającego muszą posiadać możliwość otwarcia pomieszczeń, do których posiadają nadane uprawnienia.

Podstawowym zadaniem systemu kontroli KD dostępu jest czuwanie nad autoryzacją osób poruszających się. System KD musi zapewnić identyfikację osób wchodzących do chronionego obszaru a następnie, stosownie do uprawnień posiadanych przepustek, podjąć decyzję o udzieleniu dostępu. Od systemu kontroli dostępu oczekuje się wysokiej trwałości, niezawodności, dużej odporności na trudne warunki atmosferyczne oraz akty sabotażu.

System kontroli dostępu spełnia następujące zadania:

1) kontrola dostępu personelu do z góry zdefiniowanych stref KD na danym obszarze;
2) zabezpieczenie budynku lub pomieszczeń przed nieupoważnionym dostępem ;
3) zapewnienie dostępu osobom upoważnionym w odpowiednich godzinach ;
4) rejestracja karty (identyfikatora) w dzienniku ;
5) monitorowanie przemieszczania się personelu;
6) rozbrojenie/uzbrojenie systemu SSWiN.

System powinien pracować w oparciu o sieć komunikacyjną bazującą na standardzie Ethernet z protokołem TCP/IP w szczególności pomiędzy serwerem, stacjami roboczymi i kontrolerami obiektowymi - bez konwerterów pośredniczących. System powinien umożliwić podłączanie różnego typu czytników, obsługę różnych formatów kart, jak również możliwość definiowania formatów kart przez administratora systemu w celu np. umożliwienia użytkowania kart z innego systemu. System powinien być elastyczny pod względem rozbudowy i musi być zgodny z istniejącymi kartami pracowniczymi i systemami Zamawiającego.

Wykonawca zapewni szkolenie dla przedstawicieli Zamawiającego.

Oprogramowanie systemu kontroli dostępu musi umożliwiać: wprowadzanie stopniowania zakresu uprawnień poszczególnych użytkowników systemu w zależności od podania nazwy operatora i hasła dostępu; wprowadzanie/usuwanie kart dla systemu wraz z nadawaniem uprawnień dostępu oraz szerokimi możliwościami odnośnie prowadzenia bazy danych personelu; przydzielanie uprawnień poprzez nadawanie praw dostępu do pojedynczych obszarów dostępu dla pojedynczych kart jak również dla grup kart; możliwość tworzenia personelu z szablonów w celu zautomatyzowania wydawania kart; wprowadzanie harmonogramów dostępu do poszczególnych drzwi; możliwość ręcznego sterowania drzwiami (czasowe zablokowanie drzwi, czasowe otwarcie drzwi, natychmiastowe otwarcie); pełny nadzór nad zdarzeniami związanymi z użyciem karty oraz usterkami technicznymi systemu za pośrednictwem rejestru zdarzeń i okna alarmowego.

Zamawiający wymaga kontrolera współpracującego w zakresie 100% funkcjonalności z systemem Kantech. Kontroler powinien pracować w trybie klient-serwer. Kontroler powinien obsługiwać minimum 20 000 kart oraz bufor o min 20 000 zdarzeń. Każde zdarzenie, w szczególności użycie karty, otwarcie drzwi, przytrzymanie otwartych drzwi powinno zostać jednoznacznie odnotowane i przesłane do systemu centralnego Zamawiającego Veno Is z zachowaniem jego pełnej wizualizacji. System musi umożliwiać dodawanie i odbieranie uprawnień kart w czasie rzeczywistym. System musi rejestrować każde użycie karty, zarówno kart dozwolonych, jak i nieuprawnionych. Użycie karty nieuprawnionej musi zostać stosowanie wyróżnione wśród innych zdarzeń rejestrowanych.

Zamawiający wymaga aby dostarczone urządzenia współpracowały z systemem funkcjonującym już u Zamawiającego tj. oprogramowaniem „Veno Is”/”Kantech” - oprogramowanie do wizualizacji i integracji systemów zabezpieczeń mienia obejmującym następujące systemy KD, SSWiN, CCTV.

Wykonawca dostarczy licencję umożliwiającą podłączenie central alarmowych Satel do istniejącego systemu u Zmawiającego „Veno Is”.

Zamawiający prognozuje posiadać maksymalnie 20.000 unikalnych kart pracowniczych w systemie kontroli dostępu KD.

Bezpośrednio przy każdych drzwiach wyposażonych/chronionych/otwieranych za pośrednictwem systemu kontroli dostępu KD musi zostać zainstalowany punkt kontroli dostępu w postaci czytnika kart pracowniczych.

Wszystkie objęte kontrolą przejścia muszą być zarządzane z jednej konsoli, tzn. nadawanie uprawnień do poszczególnych obiektów i stref musi być wykonywane z jednego miejsca, a informacje o zmianach musza być przesyłane on-line w chwili zapisu zmian. System musi sygnalizować jakiekolwiek naruszenia w poszczególnych strefach i przesyłać wszystkie zdarzenia on-line w czasie rzeczywistym do systemu centralnego Zamawiającego. Wszystkie przejścia uwzględnione w postępowaniu muszą być zaprezentowane na mapach sytuacyjnych z rozmieszczeniem poszczególnych elementów systemów („Veno Is”/”Kantech”).

System musi sygnalizować zaistniałe zdarzenia m.in. awarie, incydenty, naruszenia prezentując takie informacje w czytelnej formie graficznej wraz z możliwością wyświetlenia szczegółowych informacji.

Zgodnie z założeniami system KD obejmuje instalację urządzeń oraz instalację kablową dla pojedynczych przejść kontroli dostępu - drzwi (realizujących ruch dwukierunkowy). Sterowanie drzwiami należy zrealizować za pomocą elektrozwory oraz czytnika zbliżeniowego.

Funkcje jednostek centralnych pełnią kontrolery dostępu, które zbierają dane z czytników kart i po pozytywnym zweryfikowaniu karty zwania elektrozworę umożliwiając wejście do wydzielonej strefy.

System kontroli dostępu KD musi rejestrować wszystkie zdarzenia, które zostały zarejestrowane przez kontrolery, a w szczególności: odczyt karty, otwarcie drzwi.

Kontroler systemu KD musi pracować w połączeniu z systemem centralnym Zamawiającego/serwerem, w przypadku utraty łączności z serwerem – autonomicznie umożliwiając identyfikację oraz weryfikację użytkowników na podstawie ostatnio zsynchronizowanej bazy danych. Po przywróceniu łączności z serwerem centralnym kontroler musi zsynchronizować wszystkie dane (m. In. wysłać zdarzenia, odebrać zmiany w bazie). Komunikacja z wykorzystaniem protokołu TCP/IP - elementy systemu komunikują się poprzez TCP/IP, co ułatwia integrację rozwiązania z istniejącą infrastrukturą informatyczną. Praca programu/systemu z różnymi bazami danych SQL - system musi dać możliwość wykorzystania różnych systemów zarządzania bazami danych, umożliwiając wykorzystanie systemu w małych oraz dużych środowiskach.

Automatyczna identyfikacja użytkownika - System przeprowadza identyfikację użytkownika bez dodatkowych akcji wykonywanych przez użytkownika. Współpraca z różnymi rodzajami kart zbliżeniowych - system daje możliwość w zależności od zastosowanego modelu terminala na współpracę z co najmniej trzema rodzajami kart zbliżeniowych (Mifare, Unique, HID).

Zamawiający wymaga odczytu/weryfikacji wszystkich bajtów karty przez cały System oraz aby karty wprowadzane i interpretowane były w Systemie zgodnie z ich prezentacją na karcie heksadecymalnie (FF FFFF FFFF FFFF).

Wbudowany interfejs Wiegand - system umożliwia integrację z istniejącymi rozwiązaniami, np.: w postaci innych czytników kart zbliżeniowych.

Praca w trybie weryfikacji i identyfikacji - system umożliwia uwierzytelnienie użytkownika na podstawie identyfikatora użytkownika.

Bieżące monitorowanie systemu - operator systemu ma możliwość ciągłego podglądu zdarzeń w systemie: rejestracji użytkowników, działań administracyjnych oraz stanów połączeń między elementami systemu.

Zarządzanie terminalami z poziomu serwera oznaczają m. in.: dodawanie użytkowników, usuwanie użytkowników, przypisywanie użytkowników do wybranych: grup, terminali, stref czasowych i in. Możliwość zaprogramowania przedziału czasowego, w którym użytkownik jest uprawniony do korzystania z terminala (dla każdego użytkownika z osobna i dla grupy). Oznacza to, że użytkownik/grupa powinien mieć dostęp do przejścia w określonym przedziale czasowym.

Możliwość ustawienia harmonogramu pracy systemu - programowanie stanu kontrolera (otwarty, zamknięty) dla odpowiedniego przedziału czasu, dni roboczych i świątecznych. Oznacza to automatyczne odblokowanie określonych drzwi w odpowiednim czasie i automatyczne zablokowanie po upływie tego terminu. Filtrowanie dziennika zdarzeń – system daje możliwość filtrowania dzienników zdarzeń według różnych kryteriów, z rozróżnieniem pozytywnych jak i negatywnych zdarzeń. Kryteria filtrowania m.in. według: grup, terminala, użytkownika, rodzaju zdarzenia, odwiedzających.

Kontrolery i czytniki muszą mieć funkcję Anti-Pass Back.

System musi mieć możliwość utworzenia planu sytuacyjnego na podstawie umieszczonych czytników do Kontroli Dostępu. Dostarczany system KD musi umożliwiać współpracę z urządzeniami m.in. kołowrotki, furtki, bramy i szlabany współpracujące z odpowiednimi czytnikami/kontrolerami itd.). Dostawca w ramach projektu musi dostarczyć wszystkie niezbędne funkcjonalności systemu - kompletne oprogramowanie i licencje zapewniające realizację wszystkich opisanych funkcjonalności.

Przy projektowaniu systemów kontroli dostępu należy uwzględnić przepisy ppoż. szczególnie mając na względzie aspekty ewakuacji, doboru klamek, dźwigni, rygli, czujników itp.

2. Parametry urządzeń

1) KONTROLER KT-1-PCB:

a) modułowy kontroler dostępu obsługą 1 przejścia dwustronnego
b) Port czytnika Wiegand, ABA Track 2,
c) Porty komunikacyjne RS232, RS485, TCP,
d) Pamięć kart 100000
e) Pamięć zdarzeń 20000
f) Liczba linii dozorowych 4
g) Liczba wyjść sterujących 2
h) zasilanie 12VDC/2A
i) Pojemność pamięci FLASH 256 MB
j) Pojemność pamięci SDRAM 128MB
k) Tryb autonomiczny
l) gwarancja: 3 lata;

2) CZYTNIK ZBLIŻENIOWY BEZ KLAWIATURY HID R10:

a) obsługa kart:
- MiFare Classic,
- MiFare Plus X (2KB EEPROM, 7bajtowy unikatowy nr seryjny),

b) interfejs Wiegand lub interfejs RS485,
c) częstotliwość komunikacji 13,56MHz,
d) zasilanie 5-16VDC
e) stopień ochrony: IP65,
f) temperatura pracy: -25°C do 50°C,
g) odporność na promieniowanie UV,
h) gwarancja: 3 lata;

3) Zasilacz

a) obsługa akumulatorów 12V zabezpieczenie przed przepięciem,
b) regulacja napięcia ładowania akumulatora, styki informujące o stanie:
c) napięcia DC,
d) napięcia AC,
e) stanie baterii,
f) gwarancja: 3lata;

4) Okablowanie

Instalacje należy wykonać zgodnie z postanowieniami obowiązujących norm, przepisów i wytycznych oraz zaleceniami producenta poszczególnych systemów. Sposób układania kabli teletechnicznych uzależnić od innych instalacji elektrycznych w obiekcie. Kable powinny być chronione przed uszkodzeniami poprzez ułożenie ich w korytkach PCV. Przy układaniu kabli zachować jak największe możliwe odległości od innych instalacji elektrycznych. System zasilić z tablicy bezpiecznikowej, poprzez wydzielony i oznaczony obwód. Linie zasilającą zabezpieczyć oddzielnym bezpiecznikiem.

Instalacja powinna być przeprowadzona przez wykwalifikowany i przeszkolony personel.