W oparciu o art. 99, ust. 5, Ustawy z dnia 11 września 2019 r. Prawo Zamówień Publicznych wskazano w  
Opisie Przedmiotu Zamówienia, znak towarowy i rozwiązania firmy UNICARD Systems Sp. z o.o. jako wzorzec funkcjonalno-jakościowy przedmiotu zamówienia. Oznacza to tym samym, że Zamawiający dopuszcza złożenie oferty na sprzęt o parametrach funkcjonalnych i jakościowych tożsamych z parametrami sprzętu określonego we wzorcu, o ile jednocześnie zostaną zachowane pozostałe wymagania, określone w SIWZ i zaoferowany sprzęt będzie równoważny pod kątem jakościowym i funkcjonalnym.

Wykazanie równoważności złożonej oferty leży po stronie Wykonawcy i powinno zostać udokumentowane w możliwie najbardziej obiektywny sposób.

**Ogólne założenia projektowe – kontrola dostępu w budynku Administracyjnym – poziom 1 piętra**

* Obecnie na poziomie 1 Piętra w budynku Administracyjnym Szkoły Podoficerskiej Państwowej Straży Pożarnej w Bydgoszczy planowany jest remont, w trakcie którego zaplanowano wdrożenie systemu kontroli dostępu,
* Projektuje się zabezpieczenie jednostronnym systemem kontroli dostępu 5 wejść do pomieszczeń.
* Wejście do każdego z wyznaczonych pomieszczeń ma zostać zabezpieczone poprzez instalację jednofunkcyjnych czytników kart zbliżeniowych bez klawiatury**.**
* Projektuje się instalację 1 szt. sieciowej centrali systemu kontroli dostępu U-700 oraz 2 szt. modułów rozszerzeń I/O-700 komunikujących się z centralą główną poprzez magistralę komunikacyjną CAN,
* Sterowniki kontroli dostępu muszą posiadać możliwość konfiguracji pracy bi-stabilnej tj. jedno zbliżenie uprawionej karty odblokowuje drzwi na stałe – na czas odblokowania drzwi dioda na czytniku zmienia kolor na zielony, drugie zbliżenie uprawnionej karty ponownie blokuje drzwi.
* Dostawa i montaż 3 szt. zasilaczy buforowych z podtrzymaniem akumulatorowym 7Ah,
* Zarządzanie uprawnieniami kontroli dostępu do nowych zabezpieczonych pomieszczeń musi się odbywać z poziomu posiadanego przez Zamawiającego oprogramowania kontroli dostępu UniKD.
* W kosztorysie należy uwzględnić wykonanie kompletnego okablowania zasilającego 230 VAC / 12 VDC oraz komunikacyjnego LAN/CAN do wszystkich urządzeń wchodzących w skład systemu,
* Celem zapewnienia komunikacji pomiędzy centralą systemu kontroli dostępu a serwerem, na którym Zamawiający posiada zainstalowane oprogramowanie do zarządzania systemem kontroli dostępu UniKD, centralę należy podłączyć przewodowo do sieci lokalnej LAN Zamawiającego. Najbliższy punkt, w którym można podłączyć centralę systemu kontroli dostępu do sieci LAN należy uzgodnić z Zamawiającym.
* W ramach realizacji projektu - drzwi do wszystkich 5 szt. pomieszczeń w budynku Administracyjnym na poziomie 1 piętra, na których planuje się uruchomienie systemu kontroli dostępu należy wymienić na nowe.
* Drzwi muszą zostać wyposażone przez producenta stolarki drzwiowej w elektro-rygle rewersyjne 12 VDC**,** zestawy pochwyt-klamka oraz samozamykacze drzwiowe.
* Zamawiający wymaga udzielenia 5 letniej gwarancji na dostarczone elementy rozbudowywanego systemu kontroli dostępu.

**Kontrola dostępu – zasady działania systemu:**

Kontrola dostępu należy do najczęściej wdrażanych systemów bezpieczeństwa. System kontroli dostępu, umożliwia ograniczenie dostępu do wybranych pomieszczeń lub stref oraz wizualizację stanów zagrożenia na terenie obiektów. System musi współpracować z systemem rejestracji czasu pracy RCP – który Zamawiający planuje wdrożyć w późniejszym terminie - w obszarze wspólnej karty RFID oraz wspólnej bazy danych MS-SQL.

Modułowy sposób budowy systemu zapewniający łatwiejszą rozbudowę o kolejne punkty sterujące drzwiami, bramkami obrotowymi, windami lub szlabanami zapewnia wykorzystanie odpowiednio dobranych sterowników spełniających minimalne parametry techniczne zawarte w poniższych tabelach.

Dostarczone rozwiązanie musi zapewniać bardzo wysoki poziom bezpieczeństwa oraz umożliwiać wykorzystanie używanych przez Zamawiającego Elektronicznych Legitymacji Służbowych Strażaka Państwowej Straży Pożarnej, zawierających moduł zbliżeniowy w technologii MIFARE DESFire, które Zamawiający koduje przy użyciu kodera UKM-900-DESFire indywidulanymi kluczami bezpieczeństwa uniemożliwiającymi wykonanie kopii lub klonu nośnika. Prócz wykorzystania w/w kart dostarczony system musi być wyposażony w urządzenia i aplikacje wykorzystujące szyfrowaną transmisję minimum AS128.

Wszystkie punkty systemu kontroli dostępu muszą być skomunikowane z serwerem oraz dedykowanymi komputerami PC na których jest obecnie zainstalowane oprogramowanie UniKD zarządzające systemem, przy użyciu sieci Ethernet. Każdy punkt kontroli dostępu musi mieć możliwość programowego sterowania z dowolnego komputera na którym zainstalowane jest oprogramowanie UniKD zarządzające systemem kontroli dostępu.

Sterowniki systemu kontroli dostępu powinny mieć możliwość: aktualizacji firmware, przechowywania w swojej pamięci wszystkich zdarzeń zaistniałych w systemie, a w szczególności: naruszenie czujnika sabotażowego czytników i sterownika, stan kontaktronu, nr karty, tryb rejestracji wejście/wyjście, datę i godzinę rejestracji.

W pamięci centrali głównej lub sterownika muszą znajdować się wszystkie uprawnienia i ograniczenia dla kart funkcjonujących w systemie w celu zapewnienia poprawnej pracy i weryfikacji uprawnień   
w przypadku utraty łączności z komputerem zarządzającym.

Sterowniki kontroli dostępu powinny przechowywać numery kart zastrzeżonych, tj. takich, których użytkownicy stracili uprawnienie do dostępu do strefy chronionej przez punkt kontroli dostępu, a nie ma dostępu do ich kart identyfikacyjnych (nie zostały oddane lub je utracono przed upłynięciem daty ważności). Ponadto centralki będą sprawdzać ważność uprawnienia do dostępu do danej strefy i automatycznie blokować dostęp, gdy minęła data ważności, uprawnienie jest w danej chwili nieważne lub numer karty znajduje się na liście kart zastrzeżonych.

W ramach realizacji systemu, Wykonawca musi doprowadzić do każdego z punktów kontroli dostępu zasilanie 230VAC oraz sieć LAN w porozumieniu z działem IT Zamawiającego.

* **Funkcje systemu kontroli dostępu**

System kontroli dostępu musi umożliwiać realizację następujących funkcji:

1. Umożliwiać definiowanie nielimitowanej drzewiastej struktury firmy   
   z możliwością przydzielenia pracowników do każdego elementu drzewa,
2. Zakładać i aktualizować bazę danych systemu (operatorzy, użytkownicy, karty, profile uprawnień itp.)
3. Zarządzać poszczególnymi punktami kontroli dostępu monitorując on-line stan poszczególnych punktów systemu kontroli dostępu,
4. Zarządzać uprawnieniami operatorów oprogramowania systemu kontroli dostępu z możliwością podziału dostępu do poszczególnych opcji systemu
5. Tworzyć raporty ze wszystkich zdarzeń systemu z możliwością filtrowania wg: zadanego przedziału czasowego, nr kart, użytkowników, wybranych punktów kontroli dostępu, trybie rejestracji, numerze strefy
6. Zobrazowanie użycia karty w postaci wyświetlenia zdjęcia użytkownika przypisanego do nr karty
7. Definiowanie stref czasowych oddzielnie dla każdego dnia tygodnia w różnych przedziałach czasowych
8. Posiadać moduł obsługi gości, który pozwala ewidencjonować ruch gości po terenie firmy. Moduł musi mieć możliwość wpisania do bazy danych systemu kontroli dostępu następujących danych: *imię, nazwisko, nr dowodu tożsamości, nr rejestracyjny pojazdu, nr przydzielonej karty, profil uprawnień.*
9. Przeglądanie zarejestrowanych zdarzeń wykonywanych przez użytkowników aplikacji
10. Umożliwienie zarządzania dostępem do wind, dostęp do każdego piętra na podstawie uprawnień.
11. **Wieloprofilowość – możliwość przypisania osoby do jednego lub wielu profilu uprawnień**
12. **Możliwość rejestracji pracy całego systemu, wywoływania pewnych akcji po wystąpieniu określonych zdarzeń, np. wyświetlenie komunikatu na ekranie programu, uruchomienia sygnału dźwiękowego w przypadku próby sforsowania drzwi.**
13. **Filtrowanie odczytów (rejestracji zdarzeń), przeglądanie ścieżek przejścia pracowników, stany osobowe stref,**
14. **Współpracę systemu z centralką alarmową i p.poż.,**
15. **Sygnalizacja forsowania drzwi – sprzętowa i w oprogramowaniu, w tym możliwość współpracy z zewnętrznym systemem dozorowym,**
16. **Odczytywanie rejestracji w sposób ciągły zapewniający stały dostęp do aktualnych zdarzeń w kontrolowanym systemie, a także o określonych, dowolnie zdefiniowanych godzinach (np. dwa razy na dobę). System po rozpoczęciu komunikacji okresowej ma przeprowadzać pobieranie danych zgromadzonych na urządzeniach do momentu opróżnienia lokalnych buforów danych na każdym z urządzeń**
17. **Umożliwienie kontroli pracy systemu, nadawania uprawnień poszczególnym użytkownikom, modyfikację reguł dostępu do określonych pomieszczeń, sporządzanie raportów,**
18. **Możliwość stałego zablokowania lub odblokowania drzwi przez operatora w dowolnym przedziale czasu,**
19. Oprogramowanie do zarządzania systemem kontroli dostępu musi być oprogramowaniem umożliwiającym integrację z systemem rejestracji czasu pracy - **przy wykorzystaniu tych samych kart elektronicznych** - na poziomie:
    * wspólnej bazy danych,
    * wspólnej bazy użytkowników systemu – identyfikowanych przez karty zbliżeniowe,
    * wspólnej bazy urządzeń, z których wybrane urządzenia mogą pełnić rolę zarówno urządzeń

Kontroli Dostępu (KD) jak i Rejestracji Czasu Pracy (RCP),

* + wspólnej listy operatorów aplikacji z możliwością wyszczególnienia poziomu dostępu,
  + wspólnej struktury firmy,
  + system ma mieć możliwość uruchomienia dodatkowej funkcjonalności w postaci dedykowanego interfejsu umożliwiającego integrację systemu z posiadanym przez Zamawiającego systemem kadrowo-płacowym

1. System kontroli dostępu ma umożliwiać rozbudowę o moduł video-rejestracji w każdym punkcie kontroli dostępu poprzez instalację zewnętrznej kamery IP, która będzie wykonywała zdjęcia użytkownikom w trakcie dokonywania rejestracji. Moduł automatycznej rejestracji zdjęć musi być zintegrowany z oprogramowaniem systemu kontroli dostępu - obsługa z tego samego okna programowego. System video-rejestracji musi zapewnić wykonywanie sekwencji zdjęć osoby zbliżającej kartę do czytnika, zdjęcia muszą być wykonane z minimum jednosekundowym interwałem czasowym. Sekwencja zdjęć musi być wykonana dla każdego zdarzenia rejestracji karty na dowolnym czytniku w systemie kontroli dostępu. Zdjęcia muszą być wykonywane symetrycznie: przed, w trakcie (jedno zdjęcie) i po zbliżeniu karty do czytnika (np. w sekwencji: 4 - 1 - 4). W oprogramowaniu systemu kontroli dostępu musi być możliwość zdefiniowania ilości zdjęć w sekwencji. System musi mieć możliwość definiowania i wykonania co najmniej 9 zdjęć w sekwencji.

* **Urządzenia systemu kontroli dostępu**

Jako najważniejszy sterownik należy zastosować tzw. główny sterownik z serii U-700 obsługujący minimum dwa przejścia chronione jedno lub dwustronnie, a prócz tego posiada możliwość rozbudowy o szesnaście modułów I/O-700 (każdy moduł obsługuje dwa przejścia jedno lub dwustronnie chronione), co daje możliwość zabezpieczenia od 2 do 34 przejść zabezpieczonych jedno lub dwustronnie. Dla zachowania najwyższego poziomu bezpieczeństwa komunikacja pomiędzy głównym sterownikiem U-700 a modułami I/O-700 należy zastosować szynę komunikacyjną CAN.

Przy instalacjach kontroli dostępu wymagających zabezpieczenia pojedynczych przejść zastosować sterowniki UC-830, autonomiczne wykorzystujące protokół komunikacyjny TCP/IP posiadające nie mniejsze możliwości niż główny sterownik U-700 oraz parametry techniczne z zakresu ilości obsługiwanych kart, ilości przechowywanych zdarzeń. Dla zachowania spójności zarządzania systemu od strony serwisowej, autonomiczny sterownik z serii UC-830 musi być konfigurowany przy pomocy strony www poprzez interfejs Ethernet.

**Ogólna charakterystyka głównego sterownika U-700**

Sterownik U-700 jest urządzeniem przeznaczonym do systemów kontroli dostępu (KD). Zaprojektowany został pod kątem średnich i dużych systemów. U-700 jest urządzeniem dwu procesorowym, dostosowanym do obsługi czterech czytników kart zbliżeniowych, pracujących w stan-dardzie ABATrack II lub Wiegand. Może obsługiwać dwa przejścia obustronnie chronione (kompletne punkty KD), standardowo wyposażone w: czytniki, rygiel lub zworę, kontaktron, przycisk otwarcia drzwi, sygnalizację akustyczno-optyczną. Urządzenie ma możliwość obsługi dodatkowych urządzeń, takich jak: syrena alarmowa, czujnik krańcowy itp.

Sterownik obsługuje maksymalnie szesnaście modułów I/O-700. Informacje o uprawnieniach przechowywane są we wspólnym buforze znajdującym się w głównym sterowniku U-700. Rozwiązanie takie znacznie podwyższa bezpieczeństwo systemu kontroli dostępu gdyż żadne dane nie są przechowywane na karcie i nie dostaną się w posiadanie osób nieuprawnionych. Ten sam bufor przewidziany jest do przechowywania wszystkich zdarzeń zachodzących na podłączonych przejściach. Sterowniki główne mogą posiadać również dwa kanały komunikacji TCP/IP oraz szynę CAN. Jeden do komunikacji z bazą danych (TCP/IP – z komputerem) drugi do komunikacji z odległymi modułami I/O-700 (CAN – długości max 1000 mb).

Sterowniki zasilane są z zasilaczy 230V AC / 12V DC z podtrzymaniem akumulatorowym, umożliwiającym pracę systemu i rejestrację wszystkich zdarzeń nawet podczas braku zasilania AC przez 12 godzin z wykorzystaniem wbudowanych bezobsługowych akumulatorów wewnątrz urządzeń. Zasilanie awaryjne umożliwia komunikację czytnika kart zbliżeniowych ze sterownikami lub modułami I/O-700 co pozwalana na pracę w trybie Off-Line.

Minimalne wymagane parametry techniczne głównego sterownika U-700 oraz modułu I/O-700 a także czytników zostały zawarte w poniższych tabelach.

**Główny sterownik U-700 wymagany do systemu kontroli dostępu o minimalnych parametrach technicznych nie gorszych niż zawarte w poniższej tabeli:**

**Tabela nr 1 - Opis minimalnych parametrów głównego sterownika systemu kontroli dostępu U700**

|  |  |
| --- | --- |
| **Opis minimalnych parametrów głównego sterownika systemu kontroli dostępu U-700** | **Wymagane Tak/Nie** |
| Napięcie zasilania: 12-14V DC | TAK |
| Płyta główna: dwuprocesorowa, oparta na technologiach AVR i ARM9 | TAK |
| Maksymalny pobór prądu: 350 mA | TAK |
| Pamięć wewnętrzna RAM: 2MB | TAK |
| Pamięć wewnętrzna Flash: 2GB / 4GB | TAK |
| Temperatura pracy: od -10 do 55 C | TAK |
| Wilgotność względna otoczenia: poniżej 80% (bez kondensacji | TAK |
| OBSŁUGA:  - 2 x złącza PKD - złącze Punktu Kontroli Dostępu (bezpośrednio max. 4 czytniki kart RFID)  - 16 x moduł I/O podłączonych za pomocą magistrali CAN  Liczba obsługiwanych punktów KD: do 34 (z wykorzystaniem modułów I/O-700) | TAK |
| Pomiar czasu: zegar czasu rzeczywistego (RTC) w systemie 24h | TAK |
| Podtrzymanie RAM’u i zegara: akumulator NiMH 2,4V / 80 mAh | TAK |
| Sygnalizacja: diody LED, sygnalizator akustyczny | TAK |
| WEJŚCIA:  - 2 x przycisk otwarcia drzwi  - 2 x kontaktron  - 4 x sabotaż czytnika  - 1 x sabotaż sterownika  - 1 x info o zasilaniu  - 1 x alarm PPOŻ (optoizolowane) | TAK |
| WYJŚCIA:  - 2 x wyjście rygiel (przekaźnik NO/NC 30V/1A)  - 2 x wyjście alarmowe (przekaźnik NO/NC 30V/1A) | TAK |
| FUNKCJONALNOŚCI  - sposoby identyfikacji przy pomocy kodu wejściowego, karty, karty i PIN-kodu, karty i PIN-kodu po godzinach,  - uprawnienia dla kart: siatka czasowa, aktywność karty, termin ważności, limit przejść (N-razy)  - harmonogram automatycznego trwałego odblokowania PKD  - rozbudowana siatka czasowa uprawnień (4 zakresy dziennie, 28 zakresów na tydzień)  - obsługa do 16 stref alarmowych (wej/wy cyfrowe)  - możliwość blokady i odblokowania przejścia karta rezydenta  - rozdzielność uprawnień ze względu na stronę PKD  - szyfrowany protokół AS128 z serwerem Ethernet (TCP/IP)  - protokół z modułami I/O - CAN  - obsługa 16 modułów I/O  - wykrywanie sabotażu centralki oraz czytników  - bi-stabilna praca punktów kontroli dostępu | TAK |
| Możliwość przechowywania uprawnień w pamięci wewnętrznej:  - 50 000 rekordów pełnych  - rozbudowana struktura uprawnień (możliwość ustawienia siatki czasowej, kodów PIN, termin ważności karty  - 100 000 rekordów podstawowych - identyfikator, wejście tak/nie  - do 1000 000 zdarzeń w pamięci Flash | TAK |
| INTERFEJSY:  - 1 x Ethernet – przeznaczony do personalizacji instalacji za pomocą strony www oraz komunikacji z oprogramowaniem zarządzającym za pomocą szyfrowanego połączenia TCP/IP  - 1 x RS-232/RS-485 – do konfiguracji sterownika  - 1 x RS-232 – do urządzeń peryferyjnych  - 1 x separowany galwanicznie interfejs CAN (do podłączenia modułów rozszerzeń I/O)  - 4 x AbaTrackII / Wiegand  - 8 x uniwersalne wejścia/wyjścia | TAK |

**Moduł I/O-700 wymagany do systemu kontroli dostępu o minimalnych parametrach technicznych nie gorszych niż zawarte w poniższej tabeli:**

**Tabela nr 2 - Opis minimalnych parametrów modułu rozszerzeń I/O-700**

|  |  |
| --- | --- |
| **Opis minimalnych parametrów sterownika I/O-700** | **Wymagane Tak/Nie** |
| Napięcie zasilania: 12-14V DC | TAK |
| Maksymalny pobór prądu: 200 mA (bez czytników) | TAK |
| Temperatura pracy: od -10 do +55 C | TAK |
| Wilgotność względna otoczenia: poniżej 80% (bez kondensacji | TAK |
| OBSŁUGA:  - 2 x złącza PKD - złącze Punktu Kontroli Dostępu (bezpośrednio max. 4 czytniki kart RFID) | TAK |
| Sygnalizacja: diody LED | TAK |
| WEJŚCIA:  4 x czytnik w formatach: standardowe – ABA-Track II / Clock&Data na zamówienie – Wiegand 26(H10301) / 58(Unicard) bitów oraz inne według specyfikacji klienta  2 x przycisk otwarcia drzwi  2 x kontaktron  4 x sabotaż czytnika  1 x sabotaż modułu  1 x info o zasilaniu  1 x alarm PPOŻ (optoizolowane) | TAK |
| WYJŚCIA:  2 x wyjście rygiel (przekaźnik NO/NC 30V/1A)  2 x wyjście alarmowe (przekaźnik NO/NC 30V/1A | TAK |
| OBUDOWA  - ABS | TAK |
| INTERFEJSY:  1 x RS-232/RS-485 – do urządzeń peryferyjnych  1 x separowany galwanicznie interfejs CAN (do komunikacji ze sterownikiem U-700)  4 x uniwersalne wejścia | TAK |

**Autonomiczny sterownik UC-830 wymagany do systemu kontroli dostępu o minimalnych parametrach technicznych nie gorszych niż zawarte w poniżej tabeli.**

**Tabela nr 3.**

|  |  |
| --- | --- |
| **Opis minimalnych parametrów sterownika systemu kontroli dostępu UC-830** | **Wymagane Tak/Nie** |
| Napięcie zasilania: 12-14V DC | TAK |
| Maksymalny pobór prądu: 300 mA (bez czytników) | TAK |
| Pamięć wewnętrzna RAM: 1MB | TAK |
| Temperatura pracy: od -10 do 55 C | TAK |
| Wilgotność względna otoczenia: poniżej 80% (bez kondensacji | TAK |
| OBSŁUGA:  - 1 x złącza PKD - złącze Punktu Kontroli Dostępu (bezpośrednio max. 2 czytniki kart RFID) | TAK |
| Pomiar czasu: zegar czasu rzeczywistego (RTC) w syst. 24h | TAK |
| WEJŚCIA:  - 1 x przycisk otwarcia drzwi  - 1 x kontaktron  - 2 x sabotaż czytnika  - 1 x sabotaż rejestratora-opcjonalne  - 1 x alarm PPOZ (optoizolowane)  - 2 x wej/wyj uniwersalne cyfrowe (opcja na zamówienie) | TAK |
| WYJŚCIA:  - 1 x wyjście rygiel (przekaźnik NO/NC 30V/1A)  - 1 x wyjście alarmowe (przekaźnik NO/NC 30V/1A)  - 1x wyjście: 12V/1A | TAK |
| Możliwość przechowywania uprawnień w pamięci wewnętrznej:  - 50 000 rekordów pełnych (karty RFID)  - rozbudowana struktura uprawnień (możliwość ustawienia siatki czasowej,  termin ważności karty)  - 100 000 rekordów podstawowych - identyfikator, wejście tak/nie  - do 1000 000 zdarzeń w pamięci Flash | TAK |
| INTERFEJSY:  - 1 x Ethernet – przeznaczony do personalizacji instalacji za pomocą strony www  oraz komunikacji z oprogramowaniem  zarządzającym za pomocą szyfrowanego połączenia TCP/IP  - 1 x RS-232 – do urządzeń peryferyjnych  - 2x Aba TrackII/Wiegand 26(H10301)/58(Unicard) lub inne na zamówienie | TAK |

**Czytnik kart zbliżeniowych UR-905 wymagany do systemu kontroli dostępu o minimalnych parametrach technicznych nie gorszych niż zawarte w poniższej tabeli:**

**Tabela nr 4 - Opis minimalnych parametrów czytnika kart UR-905 do zastosowania w systemie kontroli dostępu**

|  |  |
| --- | --- |
| **Opis minimalnych parametrów czytnika kart do zastosowania w systemie kontroli dostępu UR-905** | **Wymagane Tak/Nie** |
| Napięcie zasilania:    9-14V DC | TAK |
| Maksymalny pobór prądu:  180 mA dla zasilania 9V 140 mA dla zasilania 12V 120 mA dla zasilania 14V | TAK |
| Obsługa kart zbliżeniowych: MIFARE Plus S & X (SL3), MIFARE DESFire Pliki | TAK |
| Jednoczesna obsługa technologii RFID + NFC + Bluetooth 4.0 | TAK |
| Zasięg odczytu: do 6 cm, | TAK |
| Częstotliwość pracy: 13,56 MHz | TAK |
| Sygnalizacja: dioda LED dwukolorowa oraz sygnalizator akustyczny | TAK |
| Mechaniczny czujnik antysabotażowy: mechaniczny, styk typu NC, obciążalność max 100 mA | TAK |
| Interfejs komunikacyjny:  ABA Track II, Wiegand 26(H10301)/58 bitów oraz dwukierunkowa transmisja. | TAK |
| Klawiatura: silikonowa 12-klawiszowa (3x4) z podświetleniem (jako wersja opcjonalna) | TAK |
| Przewód podłączeniowy zespolony bezpośrednio do elektroniki wewnętrznej 10-cio żyłowy z ekranem o dł. Minimum 2,5m | TAK |
| Obudowa:  ABS - obudowa zewnętrzna  SAN - obudowa wewnętrzna | TAK |
| Stopień ochrony obudowy:    IP 65 wg EN 60529 | TAK |
| Kolory obudów:   grafit/czarny | TAK |
| Waga:    około 250 g | TAK |
| Wymiary (wys. x szer. x głęb.):    105 x 47 x 25 mm | TAK |
| Temperatura pracy:    od -25oC do +55oC | TAK |
| Temperatura przechowywania:    od -20oC do +70oC | TAK |
| Wilgotność względna otoczenia: max 100% (dopuszczalna kondensacja) | TAK |
| Układ elektroniczny scalony na stałe z obudową wewnętrzną | TAK |

**Wymagania w zakresie kart zbliżeniowych Mifare®DESFire**

Zamawiający wymaga, aby cześć zbliżeniowa wykorzystywana w systemie kontroli dostępu działała w oparciu o posiadane przez Zamawiającego Elektroniczne Legitymacje Służbowe Strażaka Państwowej Straży Pożarnej, zawierające moduł zbliżeniowy Mifare®DESFire EV1 4k. Identyfikacja powinna odbywać się na podstawie danych zapisanych w pamięci karty, do której sektorów dostęp powinien być chroniony kluczami unikalnymi dla każdej karty (dywersyfikacja kluczy). Dane na karcie powinny być zabezpieczone kryptograficznie za pomocą algorytmu AES128 oraz 3DES.

Czytniki kontroli dostępu powinny obsługiwać karty ze strukturą MAD (Mifare Application Directory), których klucze autoryzujące do danych identyfikatora są zdywersyfikowane.

**Nie dopuszcza się stosowania w systemie numeru seryjnego karty Mifare®DESFire EV1 4k jako numeru identyfikacyjnego.**

**Zestawienie urządzeń oraz usług – Kontrola dostępu Budynek Administracyjny – poziom 1 Piętra**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Opis punktu KD** | **Czytnik kart zbliżeniowych Mifare DESFire** | **Centrala główna systemu kontroli dostępu** | **Moduł rozszerzeń** | **Zasilacz buforowy 12 VDC; 2,5 A** | **Akumulator żelowy 12 VDC, 7 Ah** | **Drzwi aluminiowe z okuciami typu pochwyt - klamka** | **Elektrorygiel REWERSYJNY 12 VDC** | **Samozamykacz drzwiowy** | **Montaż stolarki drzwiowej** | **Montaż urządzeń kontroli dostępu** | **Wykonanie kompletnego okablowania zasilającego i komunikacyjnego** | **Uruchomienie systemu KD z poziomu oprogramowania UniKD** |
| 1 | Pomieszczenie nr 1 | 1 | 1 |  | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | Pomieszczenie nr 2 | 1 |  |  |  |  | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 3 | Pomieszczenie nr 3 | 1 |  | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 4 | Pomieszczenie nr 4 | 1 |  |  |  |  | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 5 | Pomieszczenie nr 5 | 1 |  | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | **RAZEM** | **5** | **1** | **2** | **3** | **3** | **5** | **5** | **5** | **5** | **5** | **5** | **5** |