Załącznik 9

**Tabela1**  
Funkcjonalności i parametry urządzeń wymagane na dzień złożenia oferty

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P.** | **Opis funkcjonalności/parametrów** | **Wartość oferowana (TAK/NIE)** | **Wartość wymagana** |
| **I. Struktura systemu, zarządzanie i konfiguracja** | | | |
| 1 | Infrastruktura systemu oparta o technologię IP. Komunikacja pomiędzy urządzeniami systemu tj. serwery, stanowiska administratorów i operatorów, kontrolery musi odbywać się za pośrednictwem sieci LAN i standardowego protokołu TCP/IP (IPv4 i IPv6). |  | TAK |
| 2 | Scentralizowana obsługa systemu umożliwiająca zarządzanie całą infrastrukturą, poświadczeniami i użytkownikami z jednego miejsca (oprogramowania). |  | TAK |
| 3 | Obsługa przez system wielu rodzajów urządzeń sprzętowych powiązanych w grupy np. kontrolery z jednym czytnikiem, kontrolery z 2 czytnikami, zintegrowane czytniki i kontrolery drzwi oraz kontrolery drzwi z włączoną funkcją Power-over-Ethernet (PoE). |  | TAK |
| 4 | Obsługa protokołu OSDP z szyfrowaniem min AES 128 bit na magistrali szeregowej RS485 |  | TAK |
| 5 | Odczytywanie obiektu SIO wgranego na kartę typu MIFARE (13,56MHz). |  | TAK |
| 6 | Globalna funkcja „antipasspback” w trybie online oraz w trybie offline w przypadku utraty komunikacji z serwerem. |  | TAK |
| 7 | Możliwość tworzenia i obsługi zdefiniowanych scenariuszy bezpieczeństwa. |  | TAK |
| 8 | Konfiguracja uprawnień dla obsługi i administracji (np. w ramach poszczególnych budynków lub grupy użytkowników lub poświadczeń) |  | TAK |
| 9 | Obsługa funkcjonalności programu przy pomocy utworzonych pulpitów nawigacyjnych. Konfiguracja powinna umożliwiać tworzenie w okienku pulpitu nawigacyjnego widżetów z możliwością określenia ich lokalizacji i rozmiaru, tytułu widżetu, koloru tła widżetu oraz możliwości okresowego odświeżania zawartości widżetu. Typami widżetów pulpitu nawigacyjnego będą: obraz - umożliwia wyświetlanie obrazu (JPG, PNG, GIF, BMP) na pulpicie nawigacyjnym. tekst - umożliwia wyświetlanie tekstu na pulpicie nawigacyjnym. Styl tekstu musi być konfigurowalny, aby użytkownik mógł określić czcionkę, rozmiar, kolor i wyrównanie tekstu.  kafelek - umożliwia wyświetlanie dowolnego obiektu z USP wewnątrz kafelka.  strona internetowa: umożliwia wyświetlanie adresu URL na pulpicie nawigacyjnym. |  | TAK |
| 10 | Oprogramowanie musi umożliwiać indywidualne ustawianie interfejsów (pulpitów nawigacyjnych) dla administratora lub użytkownika (lub grup użytkowników), w zależności od nadanych uprawnień. Wybrani użytkownicy lub grupy nie powinny mieć możliwości zmiany tych ustawień. |  | TAK |
| 11 | Nadawanie uprawnień poszczególnym użytkownikom systemu zarządzania w zależności od stanowiska (administrator, operator, portier itp.) z możliwością ograniczania uprawnień w zadanych przedziałach czasowych oraz zmiany tych uprawnień dla całej grupy. |  | TAK |
| 12 | Struktura oprogramowania musi umożliwiać dopasowanie funkcjonalności udostępnianych przez program odpowiednio do potrzeb danego stanowiska pracy (administrator, operator, portier itp.) – w zależności od użytkowanego na danym stanowisku modułu aplikacji lub/i uprawnień użytkownika. |  | TAK |
| 13 | Możliwość tworzenia polityk haseł dla użytkowników. |  | TAK |
| 14 | Pulpity nawigacyjne będą dzielone w folderze prywatnym lub publicznym. |  | TAK |
| 15 | Możliwość obsługi w przyszłości systemu rozbudowanego o kolejne przejścia minimum do 2500 przejść. |  | TAK |
| 16 | Definiowanie kalendarza świąt uwzględniającego opcję automatycznego nadawania/blokowania dostępu do wskazanych przejść lub grup przejść oraz dla wskazanych poświadczeń lub grup poświadczeń. |  | TAK |
| 17 | Oprogramowanie klienta musi zapewniać dostęp lokalny (na serwerze i stacjach operatorskich z zainstalowanym dedykowanym oprogramowaniem typu klient) oraz za pomocą zdalnego połączenia z opcją przejęcia lub podglądu stacji operatorskiej. |  | TAK |
| 18 | Aplikacja obsługująca system musi obsługiwać 64-bitowy tryb pracy. |  | TAK |
| 19 | Wszystkie aplikacje obsługujące system powinny zapewniać mechanizm uwierzytelniania i autoryzacji użytkowników. W związku z tym administrator (z odpowiednimi uprawnieniami) może zdefiniować określone prawa dostępu i uprawnienia dla każdego użytkownika w systemie. |  | TAK |
| 20 | Pełna obsługa aplikacji w języku polskim i angielskim. |  | TAK |
| 21 | Oprogramowanie zainstalowane na serwerze musi utrzymywać łącze komunikacyjne z kontrolerami sprzętowymi, w sposób ciągły monitorować, czy kontrolery są w trybie online, czy offline oraz sygnalizować stan pracy systemu, w tym na przykład brak połączenia z elementami systemu lub awarie . |  | TAK |
| 22 | Zarządzanie uprawnieniami użytkownika(karty) typu gość - np. określenie terminu ważności (od do) |  | TAK |
| 23 | Opcja aktywacji lub wyłączenia profilu posiadacza karty: aktywacja profilu posiadacza karty od zadanego czasu i daty, wygaśnięcie uprawnień w oparciu o datę pierwszego użycia poświadczeń lub wygaśnięcie w dniu zdefiniowanym przez uprawnionego użytkownika. |  | TAK |
| 24 | Grupowa aktywacja, dezaktywacja lub reaktywacja użytkowników. |  | TAK |
| 25 | Możliwość przypisania kilku kart lub poświadczeń dla pojedynczego użytkownika. |  | TAK |
| 26 | Konfiguracja grup uprawnień do przejść z jednoczesną możliwością nadawania dodatkowych, indywidualnych, uprawnień poza grupami. |  | TAK |
| 27 | Obsługa zaawansowanego zarządzania przejściami w zakresie: a) Jednoczesnego odblokowania wszystkich drzwi z danego obszaru. b) Konfigurowania trybu ponownego blokowania przejścia w momencie otwarcia drzwi, po określonym czasie lub w momencie zamknięcia drzwi. c) Określenia zasad dostępu dla innych posiadaczy kart, gdy osoba nadzorująca wejdzie na dany obszar. d) włączenia harmonogramu odblokowywania drzwi po wejściu pracownika do obiektu. e) uruchomienia harmonogramów i wyjątków od uruchomienia harmonogramów przyporządkowanych do przejść. Uruchomiony harmonogram ma określać kiedy drzwi powinny zostać automatycznie odblokowane lub zablokowane. Obsługa określonego harmonogramu odblokowania offline. Wyjątki od harmonogramów - określenie okresów, w których harmonogramy nie będą stosowane, na przykład w dni ustawowo wolne od pracy. f) Możliwości przypisania przynajmniej jednej kamery do przejścia. Materiał wizyjny musi być powiązany ze zdarzeniami dostępu do drzwi, takimi jak przyznanie lub odmowa dostępu. |  | TAK |
| 28 | Zliczanie osób i śledzenie obecności w obszarze z automatycznym alarmem w przypadku przekroczenia zdefiniowanego maksymalnego dopuszczalnej, maksymalnej liczby. |  | TAK |
| 29 | Obsługa niestandardowych pól w bazie systemu (pola definiowane przez użytkownika) a) Tworzenie i obsługa kilku pól niestandardowych. b) Stosowanie w/w pól dla posiadaczy kart, grup, poświadczeń i gości. c) Rodzaje obsługiwanych pól niestandardowych: tekst, liczby całkowite, liczby dziesiętne, daty, typ logiczny i obrazy (grafika). d) Możliwość definiowania wartości domyślnych. e) Wykorzystanie pól niestandardowych do zapytań i generowania raportów. |  | TAK |
| 30 | Możliwość zarządzenia użytkownikami podglądu zdarzeń systemu kontroli dostępu za pomocą przeglądarki www. |  | TAK |
| 31 | Oprogramowanie powinno być dostosowane do pracy w środowisku Windows Serwer Datacenter 2016 lub 2019 na maszynie wirtualnej udostępnionej przez Zamawiającego. |  | TAK |
| 32 | Możliwość logowania do aplikacji przy użyciu lokalnie przechowywanych kont użytkowników i haseł lub przy użyciu poświadczeń usługi Active Directory. |  | TAK |
| 33 | Oprogramowanie musi być oparte na otwartej architekturze umożliwiającej konfigurację i zarządzanie urządzeniami systemu kontroli dostępu pochodzącymi od różnych producentów. System powinien mieć możliwość integracji z różnymi modułami (w tym istniejący ALPR Genetec), kontrolerami, czytnikami kart i aplikacjami wchodzącymi w skład systemów innych niż oferowany (w przyszłości istniejący system KD BOSCH) w zakresie obsługi baz użytkowników i uprawnień oraz monitorowania pracy tych systemów. |  | TAK |
| 34 | Oprogramowanie zainstalowane na serwerze musi przeprowadzać synchronizację wszystkich kontrolowanych przez to oprogramowanie urządzeń kontroli dostępu, takich jak np. kontrolery obsługujące poszczególne przejścia lub moduły we/wy oraz weryfikować i rejestrować wszystkie działania i zdarzenia związane z dostępem, gdy kontrolery drzwi i moduły we/wy są w trybie online. |  | TAK |
| 35 | Synchronizacja jednostek sprzętowych musi być zautomatyzowana i przejrzysta dla użytkowników z możliwością ręcznej synchronizacji jednostek lub synchronizacji jednostek według harmonogramu |  | TAK |
| 36 | Interfejs monitorowania pracy systemu musi obsługiwać zarówno raportowanie za pomocą jednego kliknięcia w przypadku systemu kontroli dostępu i integrowanego systemu ALPR a w przyszłości systemu nadzoru wizyjnego, jak również śledzenie obszarów, kamer, drzwi, stref, posiadaczy kart, wind, jednostek LPR i innych za pomocą jednego kliknięcia. Raportowanie lub śledzenie za pomocą jednego kliknięcia ma tworzyć nowe zadanie z wybranymi jednostkami do raportowania lub śledzenia. |  | TAK |
| 37 | Wsparcie dla synchronizacji posiadaczy kart i grup posiadaczy kart za pośrednictwem usługi Active Directory, w tym poświadczeń i zdjęć posiadaczy kart. Możliwość importowania posiadaczy kart z usługi Azure AD. |  | TAK |
| 38 | Zapewnienie przepływu zadań dotyczących wydawania identyfikatorów i wniosków o kartę. |  | TAK |
| 39 | Natywne tworzenie poświadczeń mobilnych w oparciu o technologię SIO i zarządzanie nimi w taki sam sposób, jak innymi poświadczeniami. |  | TAK |
| 40 | Możliwość drukowania identyfikatorów i tworzenie szablonów z obsługą drukowania masowego identyfikatorów dwustronnych. |  | TAK |
| 41 | Zliczanie osób, śledzenie obecności w obszarze i obsługa zbiórki w przypadku alarmu pożarowego. |  | TAK |
| 42 | Wsparcie konfiguracji urządzenia za pomocą wstępnie skonfigurowanego szablonu przejść. |  | TAK |
| 43 | Automatyczne wykrywanie dołączanych urządzeń i ich rodzajów z wykorzystaniem dedykowanych portów. |  | TAK |
| 44 | Możliwość wymiany urządzenia (np. istniejącego kontrolera na nowy) z jednoczesnym przechowaniem dzienników i zdarzeń ze starej jednostki. |  | TAK |
| 45 | Możliwość wstępnej konfiguracji systemu przed fizyczną instalacją sprzętu. |  | TAK |
| 46 | Możliwość zbiorczej aktualizacji oprogramowania układowego |  | TAK |
| 47 | Unifikacja zarządzaniem systemami kontroli dostępu, nadzoru wizyjnego i LPR  a) Interfejs monitorowania powinien przedstawiać rzeczywisty zunifikowany interfejs bezpieczeństwa do monitorowania i raportowania ACS, VMS i ALPR. Zaawansowany podgląd na żywo i odtwarzanie zarchiwizowanych materiałów wizyjnych będzie możliwe za pośrednictwem interfejsu monitorowania.  b) Interfejs konfiguracji powinien przedstawiać rzeczywisty zunifikowany interfejs bezpieczeństwa do konfiguracji i zarządzania ACS, VMS i ALPR. c) Użytkownik będzie mógł powiązać jedną lub więcej kamer wideo z następującymi typami jednostek: obszary, drzwi, windy, strefy, alarmy, panele antywłamaniowe, kamery LPR i inne. d) Możliwość implementacji w systemie dedykowanych kamer monitoringu wizyjnego. Korelacji przesyłanego i nagranego za ich pomocą obrazu z wybranymi zaistniałymi w systemie zdarzeniami dla danego przejścia (także ALPR). |  | TAK |
| 48 | System musi docelowo umożliwiać wsparcie i możliwość integracji innych systemów zewnętrznych. Powinien zawierać funkcje i cechy umożliwiające obsługę dodawanych w przyszłości nowych elementów do integracji z systemami zewnętrznymi, takimi jak:  a) zewnętrzne systemy nadzoru wizyjnego, b) zewnętrzne systemy kontroli dostępu (w szczególności istniejący system KD firmy BOSCH), c) integracja LPR z kasami parkingowymi,  d) systemy zarządzania budynkiem, e) środowisko kontroli dostępu (skaner identyfikatorów, synchronizacja kart, Guardtour), f) protokoły danych (modbus, BacNet, OPC, SNMP), g) ściana wizyjna, h) systemy zarządzania zasobami ludzkimi (HRMS). |  | TAK |
| 49 | Dla zapewnienia odpowiedniego poziomu i ciągłości pracy system KD musi umożliwiać:  a) Zapewnienie dynamicznej rezerwy zarządzania systemem – możliwość natychmiastowej gotowości do przejęcia przez serwer zapasowy roli serwera podstawowego. Przełączenie awaryjne musi nastąpić w czasie krótszym niż 1 minuta bez działania użytkownika. b) Redundancję na poziomie katalogów z konfiguracją oraz kontrolerów obsługujących przejścia. c) Synchronizację katalogu rezerwowego bazy danych konfiguracji z katalogiem podstawowym. d) Samokontrolę i automatyczna synchronizację katalogów z opcją odzyskiwania i synchronizacji odzyskanych danych po awarii. Synchronizacja baz danych konfiguracji powinna odbywać się przy użyciu mechanizmu tworzenia kopii zapasowych i przywracania z możliwością ustawienia okresu synchronizacji. |  | TAK |
| 50 | W przypadku rozszerzenia systemu o obsługę dodatkowych modułów wizyjnych system powinien umożliwiać synchronizację baz danych konfiguracji w czasie rzeczywistym za pomocą funkcji SQL Mirroring lub SQL Always On. |  | TAK |
| 51 | System musi umożliwiać unieważnienie poświadczeń kontroli dostępu z możliwością zwolnienia nieużywanego rekordu, bez kasowania danych z zachowaniem rekordów historycznych. |  | TAK |
| 52 | W przypadku utraty połączenia z serwerem system musi zapewniać ciągłość pracy kontrolerów, modułów drzwiowych i czytników i zapisywanie zdarzeń, logów z przejść podłączonych do tych jednostek. |  | TAK |
| 53 | System ma zapewniać zapisywanie konfiguracji dla kontrolera, grup kontrolerów, grup modułów drzwiowych i łatwe zaimplementowanie konfiguracji w przypadku awarii kontrolera, a także przeniesienie ustawień konfiguracji grup przejść zależnych od danego kontrolera do innego kontrolera w celu zachowania ciągłości pracy. |  | TAK |
| **II. Monitorowanie pracy systemu, alarmy i raportowanie** | | | |
| 1 | Monitorowanie zdarzeń bieżących i ich odtwarzanie w czasie rzeczywistym. |  | TAK |
| 2 | Zarządzanie alarmami w czasie rzeczywistym. |  | TAK |
| 3 | Raportowanie oraz tworzenie niestandardowych szablonów raportów w oparciu o skonfigurowane pulpity zadań. |  | TAK |
| 4 | Interfejs systemu ma umożliwiać dostęp do monitorowania jego pracy obejmującego między innymi: alarmy i inne zdarzenia, monitorowanie komunikacji z poszczególnymi elementami systemu. |  | TAK |
| 5 | Możliwość wyświetlania zapisanych w systemie raportów. Wyświetlane dane następuje przez pokazanie całkowitej liczby wyników w raporcie, zestawu najlepszych wyników z raportu, albo wizualnego wykresu z danymi zawartymi w raporcie. |  | TAK |
| 6 | Funkcja automatycznego wysyłania powiadomienia (mail) w przypadku alarmu związanego z nieuprawnionym lub niezgodnym z harmonogramem użyciem wskazanego przejścia. Jeżeli przejście monitorowane będzie dodaną do systemu, dedykowaną kamerą - załączenie zdjęcia z tej kamery. |  | TAK |
| 7 | Raportowanie stanu aktualizacji oprogramowania urządzeń takich jak np. kontrolery oraz moduły drzwiowe |  | TAK |
| 8 | Obsługa nieograniczonej liczby dzienników i zdarzeń historycznych (w tym alarmy). Jedyne dozwolone ograniczenie, to ilość dostępnego miejsca na dysku twardym. |  | TAK |
| 9 | Funkcja monitorowania stanu przejścia (przewodowe). |  | TAK |
| 10 | Monitorowanie autoryzacji użytkownika/karty na przejściach bezprzewodowych |  | TAK |
| 11 | Funkcja monitorowania stanu baterii w przypadku zastosowania okuć bezprzewodowych. |  | TAK |
| 12 | 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 możliwość eksportu lub druku do plików typu pdf, html, docx, xlsx, csv. |  | TAK |
| 13 | Automatyczne raportowanie 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 możliwość eksportu lub druku do plików typu pdf, html, docx, xlsx, csv. |  | TAK |
| 14 | Automatyczne raportowanie o zdarzeniach dla danego, wskazanego pracownika oraz gościa (raportowanie za zadany okres). |  | TAK |
| 15 | Dostęp do logów operacji – monitorowanie / śledzenie operacji użytkowników. |  | TAK |
| 16 | Monitorowanie stanu technicznego. a) Monitorowanie stanu technicznego systemu, rejestracja zdarzeń związanych ze stanem i obliczanie statystyk dla poszczególnych zdarzeń. b) Obliczanie statystyk w określonym przedziale czasowym (godziny, dni, miesiące). c) Dostęp do danych związanych z monitorowaniem z poziomu raportów bieżących i historycznych. |  | TAK |
| 17 | Zarządzanie alarmami w oprogramowaniu. a) Tworzenie i modyfikowanie alarmów zdefiniowanych przez użytkownika. Obsługa nieograniczonej liczby alarmów zdefiniowanych przez użytkownika. b) Przypisanie harmonogramu lub okresu obowiązywania do alarmu. Alarm zostanie wyzwolony tylko wtedy, gdy jest aktualny dla bieżącego okresu. c) Ustawienie priorytetu alarmu i warunku ponownego włączenia. d) Ustawienie opcji wyświetlania bieżącego lub nagranego materiału wizyjnego, stopklatki lub ich połączenie po wyzwoleniu alarmu. e) Możliwość grupowania alarmów według źródła i typu. f) Określenie czasu, po którym alarm będzie automatycznie potwierdzany. g) Określenie odbiorców alarmu. Powiadomienia alarmowe są kierowane do jednego lub większej liczby odbiorców. Odbiorcom należy przypisać priorytet, który ustala kolejność odbioru alarmu. h) Zdefiniowanie trybu emisji alarmu. Powiadomienia o alarmach należy wysyłać w trybie transmisji sekwencyjnej lub jednorazowej. i) Określenie, czy wyświetlać źródło alarmu, jeden lub więcej elementów, czy stronę HTML. j) konfiguracja opcji obowiązkowego wysłania raportu dotyczącego zdarzenia podczas jego potwierdzania. k) Interfejs powinien obsługiwać powiadomienia alarmowe wysyłane na adres e-mail lub dowolne urządzenie korzystające z protokołu SMTP. l) Użytkownik powinien mieć możliwość potwierdzania alarmów, wysłania z systemu raportu o zaistniałym zdarzeniu po potwierdzeniu alarmu oraz przełączania alarmu w tryb cichy. m) Alarm powinien być skonfigurowany w taki sposób, aby pozostawał widoczny do momentu potwierdzenia. |  | TAK |
| 18 | Możliwość weryfikacji przyczyny alarmu bez jego potwierdzenia. |  | TAK |
| **III. Kontrolery** | | | |
| 1 | Możliwość obsługi min. 64 przejść przez jeden kontroler, z wykorzystaniem modułów rozszerzających. |  | TAK |
| 2 | Obsługa protokołów OSDP, bezpiecznego OSDP, Wiegand. |  | TAK |
| 3 | Obsługa czytników biometrycznych, pasków magnetycznych, czytników F/2F i jego nadzorowanych technologii. |  | TAK |
| 4 | Obsługa klawiatury oraz możliwość odczytywania zawartych w przesyłanych w komunikacji szeregowej danych informacji o dacie i godzinie. |  | TAK |
| 5 | Wbudowany układ pamięci kryptograficznej i szyfrowanie danych. |  | TAK |
| 6 | Komunikacja hosta chroniona przez TLS 1.2/1.1 |  | TAK |
| 7 | Złącze rozszerzające kontroler/IO chronione przez AES (seria 3 SIO) |  | TAK |
| 8 | Kontrola dostępu do sieci za pomocą 802.1X |  | TAK |
| 9 | Wsparcie dla OpenSSL |  | TAK |
| 10 | Możliwość zachowania danych przez okres min. 3 miesiący po utracie zasilania |  | TAK |
| 11 | Możliwość podłączenia min 4 czytników z użyciem protokołu OSDP. |  | TAK |
| 12 | Min. 6 wejść monitorujących oraz min 4 wyjścia przekaźnikowe. |  | TAK |
| 13 | Moduł wspiera łączenie aktywności innych urządzeń w obrębie systemu w celu generowania działań zaprogramowanych przez system. |  | TAK |
| 14 | Globalna funkcja „antipasspback” w trybie online oraz w trybie offline |  | TAK |
| **IV. Moduły rozszerzające** | | | |
| 1 | Obsługa protokołów OSDP v1 i v2. |  | TAK |
| 2 | Możliwość podłączenia min 2 czytników za pomocą protokołu OSDP. |  | TAK |
| 3 | Minimum 8 wejść programowalnych, minimum 1 wejście typu tamper, minimum 1 wejście awarii zasilania oraz min. 6 wyjść przekaźnikowych i obsługa min. 1 magistrali RS 485 |  | TAK |
| 4 | Wbudowany układ pamięci kryptograficznej i szyfrowanie danych, komunikacja zabezpieczona przez TLS 1.2/1.1 lub AES-256/128 |  | TAK |
| **V. Czytniki** | | | |
| 1 | Obsługa protokołu OSDP |  | TAK |
| 2 | Współpraca z kartami 13,56 MHz: - MIFARE Classic i MIFARE DESFire EV1; - iCLASS SE; - ISO14443A (MIFARE) CSN, ISO14443B CSN, ISO15693 CSN; - FeliCa™4 CSN, CEPAS4 CSN or CAN. |  | TAK |
| 3 | Czytniki kart zbliżeniowych jest kompatybilny z modelem danych Secure Identity Object™ (SIO) i wspiera poświadczenia Secure Identity Object™ (SIO) |  | TAK |
| 4 | Poświadczenia SIO mogą znajdować się na dowolnej liczbie nośników, takich jak karty zbliżeniowe iCLASS Seos, iCLASS SE, MIFARE Classic oraz MIFARE DESFire EV1. |  | TAK |
| 5 | Zaawansowane funkcje związane z pracą oraz wydajnością czytnika: a) zmiana priorytetów odczytu dla dualnych kart zbliżeniowych z podwójnym układem wysokich częstotliwości (13.56 MHz). Zmiana priorytetu jednej technologii pomaga w jej odczycie jako pierwszej w momencie zbliżenia karty do czytnika, ograniczając w ten sposób ilość odczytów drugiej technologii. b) możliwość zmiany konfiguracji związanej z obsługą konkretnych typów kart, w celu możliwości podniesienia poziomu bezpieczeństwa w przyszłości lub w przypadku migracji ze starszego standardu na nowy. c) możliwość zmiany konfiguracji jego aplikacji z wykorzystaniem konfiguracyjnych kart firmware’owych. Funkcja umożliwia zmianę funkcjonalności poprzednio zainstalowanych czytników i dostosowaniu ich do zmian w późniejszym czasie. |  | TAK |
| 6 | Czytnik powinien umożliwiać konfigurację funkcji Velocity Checking (kontrola prędkości danych) w celu zabezpieczenia przed atakami elektronicznymi, opartymi na wielokrotnych próbach uwierzytelnienia |  | TAK |
| 7 | Odczytywanie obiektu SIO wgranego na kartę typu MIFARE (13,56MHz) przez czytniki. |  | TAK |
| 8 | Zakres temperatur pracy: nie węższy niż od -30℃ do 60℃ |  | TAK |
| 9 | Klasa środowiskowa IP65 |  | TAK |
| **VI. Okucia bezprzewodowe** | | | |
| 1 | Zintegrowany multi-technologiczny czytnik zbliżeniowy z możliwością odczytu: a) numerów seryjnych procesorów kart Mifare Classic/Mifare Plus/Mifare DESFire CSN (ISO 14443A) lub danych z sektorów pamięci; b) numerów seryjnych kart iCLASS/iCLASS SE CSN (ISO 15693)/iCLASS Seos lub danych z sektorów pamięci; c) szyfrowanych danych w standardzie SIO (Secure Identity Object); |  | TAK |
| 2 | Dostępny tryb pracy typu office (dwukrotne przyłożenie transpondera otwiera drzwi na stałe i ponowne dwukrotne przyłożenie zamyka na stałe). |  | TAK |
| 3 | Przechowywanie danych użytkowników i ich kart dostępowych/kodów PIN zarówno w aplikacji odpowiedzialnej za kontrolę dostępu, jak i w sterownikach drzwiowych (dostępy poszczególnych drzwi/grup, godziny, harmonogramy czasowe, kalendarz). |  | TAK |
| 4 | Komunikacja z systemem kontroli dostępu powinna być realizowana z wykorzystaniem protokołu TCP/IP, a autoryzacja przeprowadzana przez system KD |  | TAK |
| 5 | Mechanizm klamki umożliwiający swobodne wyjście z pomieszczenia |  | TAK |
| 6 | Możliwość przechowywania w pamięci minimum 10 awaryjnych kart (używanych wyłącznie w przypadku utraty komunikacji z anteną radiową/kontrolerem drzwiowym) |  | TAK |
| 7 | Diody LED do wizualizacji stanu pracy |  | TAK |
| 8 | Standard radiowy IEEE 802.15.4 (2.4 GHz) z szyfrowaniem komunikacja 128 bitów AES |  | TAK |
| 9 | Zasilanie bateryjne – żywotność nie mniej jak 30 000 cykli |  | TAK |
| 10 | Monitorowanie stanu drzwi, użycia klamki lub otworzenia drzwi z użyciem klucza |  | TAK |

**Tabela 2**  
Dodatkowe funkcjonalności – kryterium oceny oferty

|  |  |  |
| --- | --- | --- |
| **L.P.** | **Opis funkcjonalności** | **Wartość oferowana (TAK/NIE)** |
| 1. | Automatyzacja obsługi zdarzeń/incydentów monitorowanych przez system. Możliwość jej konfiguracji przy zastosowaniu złożonych reguł działających w oparciu o dynamicznie uzyskiwane z systemu dane oraz w oparciu o interakcje z operatorami, zgodnie z przypisanymi dla nich zadaniami i uprawnieniami. Graficzny interfejs umożliwiający tworzenie reguł oraz obsługę zdarzeń przez operatora zgodnie z utworzonymi regułami. |  |
| 2. | Możliwość rozbudowy systemu w oparciu o moduły rozszerzające komunikujące się z głównym kontrolerem w oparciu nie tylko o interfejs RS485 lecz za pomocą sieci LAN przy użyciu protokołu IPv4 i IPv6. |  |
| 3. | Moduł umożliwiający implementację planów budynków (poszczególnych kondygnacji) w oparciu o dostarczone w formie cyfrowej (np. pliki dwg) i mapy online. Funkcjonalność ma umożliwiać płynną nawigację po mapach w oparciu o technologię wielowarstwową i nawigację po planach pięter z taką samą płynnością jak przy mapach GIS, przekazując w czasie rzeczywistym informacje dla operatorów o dokładnej lokalizacji alarmów i innych wybranych zdarzeń. |  |
| 4. | Funkcja raportowania zagrożeń epidemiologicznych dla pracowników lub gości dzięki korelacji zdarzeń na wybranych strefach i przejściach. Możliwość szeregowania zdarzeń dostępu według przedziału czasu i miejsca, aby zidentyfikować osoby, które były narażone na większe ryzyko kontaktu z osobą zakażoną. |  |

**Tabela 3**  
Specyfikacja oprogramowania i sprzętu.

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P.** | **Element systemu** | **Producent, nazwa, model/wersja** | **Opcjonalnie - link do strony producenta z kartą katalogową** |
| 1. | Oprogramowanie |  |  |
| 2. | Kontrolery i moduły rozszerzające |  |  |
| 3. | Czytniki |  |  |
| 4. | Okucia bezprzewodowe |  |  |
| 5. | Elektrozaczepy i elektrozwory |  |  |