ZAKŁAD KARNY W TRZEBINI
32-540 Trzebinia, ul. Słowackiego 70
tel. 32 611 59 00, fax 32 612 15 51, email: zk_trzebinia@sw.gov.pl

Załącznik nr 1

Trzebinia, dnia 15.09.2022 r.

Rozbudowa systemu nadzoru wizyjnego i kontroli dostępu na terenie Zakładu Karnego w Trzebini.

W Zakładzie Karnym w Trzebini w wybranych grupach przejść przewiduje się wykonanie instalacji systemu kontroli dostępu (KD) oraz uzupełnienie kamer do weryfikacji osób przechodzących przez podane przejścia objęte system KD (CCTV IP / VMS). System KD musi posiadać certyfikat zgodności z normą PN-EN 50133-1: 2007 dla klasy dostępu B i Grade 3.

Zaproponowany system musi posiadać możliwość wizualizacji na bazie mapy synoptycznej wszystkich zdarzeń, oraz integracji programowej z istniejącymi systemami na terenie jednostki tj. SSWiN (SATEL), CCTV IP / VMS (VDG SENSE). Jest to konieczne do realizacji Wytycznych Dyrektora Generalnego SW w celu podwójnej weryfikacji osób przemieszczających się przy wybranych przejściach KD. Ponadto w przyszłości system musi umożliwiać integrację z depozytorem kluczy oraz musi mieć możliwość rozbudowy o dodatkowe 200 czytników KD bez konieczności wymiany serwera i licencji bazowych systemu.

Kluczowy z punktu widzenia bezpieczeństwa i samej obsługi systemu jest interfejs użytkownika. Platforma musi oferować czytelny i intuicyjny interfejs użytkownika GUI znany wszystkim użytkownikom Internetu i Eksploratora Windows. W ustawieniach parametrów systemowych, każdy moduł obsługi poszczególnych systemów (kontroli dostępu, SSWiN itp.) musi mieć odmienny kolor tła, co podpowiada jednoznacznie użytkownikowi, w której części menu się znajduje.

System musi mieć wbudowaną mapę synoptyczną (wizualizację) za pomocą, której będzie istnieć możliwość pełnej wizualizacji stanu i zarządzania wszystkimi podsystemami. Funkcje, które muszą być realizowane przez system wizualizacji:

- System Kontroli dostępu – wizualizacja stanów czytnika, kontaktronu, elektrorygla i wszystkich elementów dodatkowych. Po kliknięciu ikony czytnika powinna zostać wyjustowana lista wyboru trybów pracy czytnika (m.in. stan otwarty, stan normalny, stan z potwierdzeniem operatora).
- System Sygnalizacji Włamania i Napadu – wizualizacja stanów poszczególnych elementów detekcyjnych (np. czujek ruchu PIR). Zazbrajanie i rozbrajanie poszczególnych stref SSWiN.
- System Monitoringu wizyjnego – kliknięcie ikony kamery ma spowodować wyświetlenie obrazu z danej kamery. Dla kamer PTZ, pełna możliwość sterowania kamerą z poziomu mapy synoptycznej. Możliwość umiejscowienia na mapie synoptycznej przycisków, wymuszających obrót kamery PTZ w konkretne miejsce.

Dodatkowo mapa synoptyczna musi wspierać system widgetów, który umożliwia umieszczenie na niej dowolnych elementów, m.in.:

- Listę osób znajdujących się w danym pomieszczeniu.
- Wykresy zawierające liczby osób przechodzących przez dane przejście.
- Listę stref SSWiN z informacją o ich stanie, umożliwiającą zazbrajanie i rozbrajanie poszczególnych stref.
- Skróty do konkretnych pozycji w menu, szczególnie często używanych przez operatora.
- Listę urządzeń z informacją o ich stanie połączenia z serwerem.

Kliknięcie każdej z ikon urządzenia prawym przyciskiem myszy, ma spowodować wyświetlanie wszystkich zdarzeń związanych z danym urządzeniem. Umożliwia to szybkie odwołanie do zdarzeń w obrębie każdego z systemów. Dodatkowo musi istnieć możliwość umiejscowienia bezpośrednio na mapie synoptycznej odnośnika do innej mapy synoptycznej.

Ma on objąć swoim zasięgiem wejścia główne i pomocnicze do pawilonów mieszkalnych, wszystkie przejścia (kraty) na terenie jednostki, oraz cały teren wartowni. Kontrolę dwustronną realizowaną w oparciu o jeden, lub dwa czytniki kontroli dostępu, zlokalizowane na wejściu i wyjściu do strefy należy zainstalować w ramach każdego przejścia objętego systemem Kontroli Dostępu. Przy każdym przejściu dodatkowo instalować przyciski przywołania dla osób które nie posiadają kart KD.

W drzwiach objętych systemem kontroli dostępu zostaną zainstalowane zamki elektromagnetyczne, czytniki zbliżeniowe umożliwiające otwarcie drzwi za pomocą karty oraz przyciski umożliwiające awaryjne otwarcie drzwi w przypadku ewakuacji. W ościeżnicach drzwi zainstalowane zostaną kontaktrony do sygnalizacji i rejestracji otwarcia drzwi.

Zaleca się aby Wykonawca dokonał wizji lokalnej na terenie przewidzianej inwestycji w celu uzupełnienia wszelkich informacji, które mogą być konieczne do przygotowania oferty. Podczas wizji lokalnej zostaną udostępnione do wglądu plany i schematy istniejących systemów i kanałów teletechnicznych niezbędnych do wykonania przedmiotowego zadania.

Głównym zadaniem systemu kontroli dostępu jest zarządzanie kontrolą dostępu do poszczególnych obszarów zlokalizowanych na terenie Zakładu Karnego. System KD ma uniemożliwić wejście jak i wyjście do konkretnej strefy KD osobom nieuprawnionym. System KD musi mieć możliwość definiowania harmonogramu terminowego dostępu do stref KD dla poszczególnych użytkowników lub grup użytkowników. Harmonogramy muszą mieć możliwość działania w pętli. Dodatkowo system KD musi umożliwiać definiowania harmonogramów czasowych definiujących prawa dostępu w konkretnym dniu z dokładnością do jednej minuty.

System kontroli dostępu musi również umożliwiać śledzenie i lokalizowanie osób przemieszczających się w obrębie chronionych stref. System musi mieć możliwość generowania raportów na temat ilość osób znajdujących się w poszczególnych strefach, dzięki czemu możliwa jest np. optymalizacja akcji ewakuacyjnej. Dodatkowo system powinien umożliwiać definiowanie na klawiaturze operatora klawisza szybkiego wyboru, który automatycznie generuje raport zawierający listy osób przebywających na obiekcie, z podziałem na strefy KD. System KD musi mieć możliwość sprawdzenia gdzie poszczególni użytkownicy znajdują się w czasie rzeczywistym i gdzie znajdowali się w wybranym momencie w przeszłości. Dzięki temu możliwa jest weryfikacja, np. jakie osoby znajdowały się w pomieszczeniu w momencie kradzieży mienia. Dodatkowo w oparciu o dane odnośnie liczby osób przebywających w poszczególnych pomieszczeniach, system umożliwia rozpoczęcie automatycznych procedur, np. wyłączenie zasilania i zazbrojenie strefy SSWiN po opuszczeniu przez wszystkich użytkowników danej strefy.

System powinien być w pełni skalowalny i obsługiwać w ramach jednego serwera zarządzającego, co najmniej 100 000 aktywnych kart (użytkowników) i co najmniej 1500 grup kart. System KD musi dodatkowo wspierać co najmniej 2000 czytników oraz kontrolerów kontroli dostępu w ramach jednego serwera. Musi być możliwość podłączenia na wejścia kontrolerów co najmniej 8000 elementów zewnętrznych (przyciski wyjścia, alarmowe, kontaktrony itp.). Dzięki temu możliwa będzie bezproblemowa rozbudowa systemu KD w przyszłości. Dodatkowo musi istnieć możliwość łączenia co najmniej 100 serwerów w pełni zintegrowany system kontroli dostępu z jednym serwerem nadrzędnym.

System KD musi umożliwiać podłączenie różnorodnych typów czytników kontroli dostępu. Mogą być to zarówno czytniki przewodowe, jak i bezprzewodowe. Musi być możliwość użycia na obiekcie jednocześnie obu typów czytników. Przewodowy system kontroli dostępu musi mieć możliwość podłączenia czytników w oparciu o dwie architektury, w zależności od potrzeb inwestora i okablowania zainstalowanego już na obiekcie. W pierwszej architekturze - gwiazdy, serwer musi komunikować się z dedykowanymi sterownikami sieciowymi przez sieć TCP/IP. Każdy ze sterowników musi obsługiwać co najmniej 8 kontrolerów drzwiowych, a każdy kontroler drzwiowy co najmniej 2 czytniki. Sumarycznie w architekturze gwiazdy, sterownik musi obsługiwać co najmniej 16 czytników.

W drugiej architekturze – magistralowej, sterownik sieciowy musi komunikować się z serwerem przez sieć TCP/IP i posiadać wbudowane 4 interfejsy magistral RS-485. Do każdej magistrali musi istnieć możliwość podłączenia co najmniej 8 kontrolerów drzwiowych, każdy obsługujący co najmniej 2 czytniki. Sumarycznie w architekturze magistrali, sterownik musi obsługiwać co najmniej 32 czytniki.

Obie architektury można używać w jednym systemie. W obu przypadkach czytnik kontroli dostępu komunikuje się w czasie rzeczywistym z serwerem zarządzającym, dzięki czemu ewentualne zmiany wprowadzone w systemie (np. uprawnień) są bez opóźnień realizowane na obiekcie.

Aby zabezpieczyć bezproblemowe działanie systemu, na wypadek braku komunikacji lub uszkodzenia serwera, inteligencja musi zostać rozproszona do poziomu lokalnych sterowników. Sterowniki muszą być wyposażone w moduły pamięci pozwalające na buforowanie transakcji w przypadku braku komunikacji z serwerem centralnym (co najmniej 20 000). Dodatkowo muszą przechowywać informację na temat uprawnień poszczególnych użytkowników, dzięki czemu mogą sterować czytnikami całkowicie samodzielnie (co najmniej 5000 uprawnień). W momencie, gdy sterowniki ponownie otrzymają połączenie z serwerem, muszą zsynchronizować swoją bazę danych lokalną z serwerem centralnym (przesłanie buforowanych zdarzeń, aktualizacja uprawnień).

System KD musi umożliwiać podłączenie szerokiego zakresu czytników kontroli dostępu. System kontroli dostępu musi mieć możliwość komunikacji z czytnikiem za pomocą protokołów Wiegand, Clock&Data lub RS-422 w zależności od stosowanego sterownika. System musi obsługiwać czytniki wspierające szeroki zakres technologii zbliżeniowych, m.in. krótkiego zasięgu - Legic Prime, Legic Advant, Mifare (1K, 4K), Mifare DESFire, Mifare DESFire EV1,Mifare PLUS X, Unique, iClass, jak i dalekiego zasięgu – HyperX, czy UHF.

System KD musi mieć również możliwość obsługi gości. System musi umożliwiać dodanie przez użytkowników do systemu informacji o przyjeździe gościa, którą otrzymuje operator systemu. Dodatkowo musi być możliwość przypisania do danej osoby numeru rejestracyjnego samochodu. Operator musi mieć możliwość przygotowania dla gościa specjalnej, spersonalizowanej karty z tymczasowymi prawami dostępu do wyznaczonych pomieszczeń, gdzie mają miejsce spotkania.

Komunikacja między serwerem centralnym a sterownikiem kontroli dostępu musi się odbywać w oparciu o protokół TCP/IP. System musi umożliwiać realizację szyfrowania za pomocą standardu AES-CBC (256 bit) (wykorzystując odpowiedni sterownik). Dla każdej sesji musi być generowany nowy klucz, aby zapobiec powtórzeń kluczy. Klucze muszą być zapisane w pliku XML, który musi być zabezpieczony za pomocą szyfrowania AES-256.

System KD musi zabezpieczać przed niewłaściwym użyciem karty przez użytkowników oraz sygnalizować sytuacje alarmowe. W tym celu musi realizować poniższe funkcjonalności:

- Funkcję globalnego Anti-Pass Back z podziałem na strefy (wsparcie dla Anti-Pass Back globalnie, punktowo, czasowo, rewersyjnie).
- Funkcję śluzowości obsługującą do 16 przejść.
- Funkcję unieważniania kart zbyt długo nie używanych zabezpieczające przed użyciem zagubionej karty, np. karta nie użyta na jednym z czytników w ciągu 24 godzin traci swoje prawa dostępowe.
- Funkcję kwarantanny, która zabrania użytkownikom wejście do określonych stref, jeżeli wcześniej znajdowali się w innej, ściśle zdefiniowanej strefie.

- Funkcję nadawania praw użytkownikom, w momencie gdy znajdowali się w innej strefie, np. karta jest ważna na terenie magazynu, tylko w momencie gdy wcześniej została użyta w portierni.
- Element ryglujący musi dokonywać zaryglowania przejścia niezwłocznie po zamknięciu drzwi przez osobę wchodzącą do pomieszczenia (element ryglujący nie czeka, aż skończy się czas odryglowania ustawiony w systemie).
- Funkcję wzbudzenia alarmu w momencie gdy drzwi na zbyt długi czas pozostają otwarte.
- Funkcję wejścia pod przymusem polegającą na zapisaniu dla danego użytkownika dwóch haseł pin. W momencie gdy dany użytkownik wchodzi pod przymusem do strefy, przykłada kartę i wpisuje hasło dedykowane dla wejścia pod przymusem. Uzyskuje on dostęp do danej strefy, jednocześnie operator zostaje powiadomiony o fakcie wejścia pod przymusem.
- Funkcję rozbudowanych alarmów kontroli dostępu, w których alarm jest wzbudzony w momencie gdy karta zostaje uznana jako skradziona, lub użytkownik przyłoży do kartę do czytnika do którego nie ma uprawnień.

System musi umożliwiać zmianę stanu przejścia. W systemie muszą być wyróżnione następujące tryby pracy przejścia kontroli dostępu:

- Otwarte – element ryglujący jest nieaktywny;
- Normalny – kontrola dostępu zgodna z harmonogramem i uprawnieniami użytkowników;
- Zablokowany – element ryglujący zaryglowany, czytnik zablokowany i nie odczytuje kart dostępowych;
- Z potwierdzeniem – W momencie gdy użytkownik przykłada kartę dostępową operatorowi prezentowane jest okno w którym widoczne jest zdjęcie właściciela karty z bazy systemowej oraz obraz z kamery (w przypadku integracji systemu CCTV). Operator potwierdza czy dana osoba może wejść do danej strefy kontroli dostępu.
  Uprawniony operator musi mieć możliwość zmiany w czasie rzeczywistym trybu pracy danego czytnika kontroli dostępu z poziomu mapy synoptycznej. System musi dodatkowo mieć możliwość zmiany trybu pracy czytnika w zależności od stanu systemu (stan systemu normalny, alarmowy itp.).

Wszystkie zdarzenia mające miejsce w systemie są zapisywane w bazie danych systemu. System umożliwia pełne raportowanie i archiwizację danych. System musi mieć wbudowane predefiniowane raporty, m.in:

- Raport obecności dla danego użytkownika i dla danego obszaru.
- Raport praw dostępu dla użytkownika i czytnika.
- Raport ścieżki użycia karty na obiekcie.
- Raport stanu sterowników i podłączonych do nich urządzeń.
- Raport kart według grup kart.
- Raport kart według typu kodowania.

  Dodatkowo w systemie musi być dostępny generator raportów, który umożliwia generowanie dowolnych raportów według wymogów operatora.

System kontroli dostępu powinien być również dostosowany do obsługi przez osoby niepełnosprawne, przez wydłużenie czasu zwolnienia elementu ryglującego w momencie przyłożenia karty przez osobę niepełnosprawną. Dzięki temu osoba niepełnosprawna może bez problemów przemieszczać się po obiekcie.

System musi mieć wbudowaną mapę synoptyczną (wizualizację) za pomocą, której będzie istnieć możliwość pełnej wizualizacji stanu i zarządzania systemem kontroli dostępu. Funkcje, które muszą być realizowane przez system wizualizacji: wizualizacja stanów czytnika, kontaktronu, elektrorygla i wszystkich elementów dodatkowych. Po kliknięciu ikony czytnika powinna zostać wyjustowana lista wyboru trybów pracy czytnika (m.in. stan otwarty, stan normalny, stan z potwierdzeniem operatora).

Opis kluczowych elementów systemu Kontroli dostępu

Sterownik sieciowy

Elementami wykonawczymi systemu kontroli dostępu muszą być inteligentne sterowniki sieciowe pozwalające na podłączenie kontrolerów drzwiowych. Sterownik musi komunikować się z serwerem za pomocą standardu TCP/IP. W przypadku zerwania łączności kontrolera sieciowego z serwerem, musi on nadal zarządzać elementami do niego podłączonymi. Dodatkowo musi zarejestrować w pamięci, co najmniej 5000 zdarzeń. Po ponownym podłączeniu go do serwera musi nastąpić automatyczna, wzajemna synchronizacja.

Sterownik sieciowy musi umożliwiać podłączenie 32 kontrolerów drzwiowych lub kontrolerów . Każdy kontroler musi być niezależnie podłączany do sterownika sieciowego przez port RJ-45. Jeden sterownik sieciowy musi obsłużyć co najmniej 16 czytników kontroli dostępu za pomocą kontrolerów drzwiowych.

Kontroler drzwiowy

Kluczowym urządzeniem wykonawczym systemu kontroli dostępu musi być kontroler drzwiowy odpowiedzialny za zabezpieczenie dwóch przejść pojedynczych lub jednego przejścia podwójnego.

W zależności od charakterystyki poszczególnych obiektów, kontroler drzwiowy musi działać zarówno w topologii gwiazdy, jak i magistrali w zależności od stosowanego typu sterownika sieciowego. Musi istnieć możliwość stosowania obu topologii jednocześnie w ramach pojedynczej instalacji, dzięki czemu istnieje możliwość dostosowania sposobu instalacji do wymogów poszczególnych pomieszczeń. Elastyczność topologii umożliwia również wykorzystanie dotychczasowego okablowania zainstalowanego już na obiekcie.

Kontroler musi obsługiwać 2 czytniki kontroli dostępu i komunikować się z nimi za pomocą protokołów Clock/Data / Wiegand. W zależności od typu architektury kontroler musi oferować 8 wejść i 4 wyjścia (gwiazda) lub 8 wejść i 8 wyjść (magistrala) do podłączenia elementów wykonawczych (kontaktronów, zwór, elektrozaczepów, przycisków wyjścia, czy przycisków ewakuacyjnych).

Kontroler musi być wyposażony w specjalny system monitorowania stanu kontrolera (autotest), umożliwiający ciągły pomiar m.in.: wewnętrznej temperatury, parametrów zasilania kontrolera i czytników oraz stanu komunikacji z czytnikami. Stan urządzenia powinien być sygnalizowany wielokolorową diodą oraz przesyłany do oprogramowania zarządzającego w czasie rzeczywistym. Dodatkowo kontroler drzwiowy musi być wyposażony w buzzer, włączany zdalnie informujący o miejscu instalacji kontrolera.

Czytniki kontroli dostępu

Czytniki kontroli dostępu muszą mieć możliwość odczytu technologii Mifare Plus X. Dodatkowo muszą mieć możliwość komunikacji za pomocą różnych protokołów transmisyjnych: Wiegand, Clock / Data, RS-485.

Wszystkie elementy elektroniczne znajdujące się wewnątrz obudowy czytnika muszą być zalewane żywicą epoksydowa. Dzięki temu czytniki są odporne na niekorzystne warunki atmosferyczne. Czytniki muszą posiadać normę szczelności IP64.