OPIS PRZEDMIOTU ZAMÓWIENIA
Dostawa i montaż systemu kontroli dostępu w budynku CIiZT PL przy ul. Nadbystrzyckiej 36C w Lublinie.

1.Ogólna koncepcja systemu

Celem instalacji systemu jest umożliwienie kontroli dostępu we wszystkich pomieszczeniach budynku przy wykorzystaniu dedykowanych kart lub legitymacji pracowniczych i studenckich.

Podczas instalacji, stosując się do przepisów ppoż, tam gdzie jest to wymagane, działanie systemu (zwolnienie blokady przejść) należy zintegrować z istniejącą centralą ppoż., tak aby w przypadku pożaru drzwi zostały automatycznie odblokowane.

Instalowany system kontroli dostępu powinien umożliwiać zarządzanie, konfigurację, raportowanie zdarzeń itp. System będzie posiadał wstępnie 160 przejść przy założeniu możliwości rozbudowy o kolejne przejścia.

Oprogramowanie obsługujące system docelowo powinno odpowiadać założeniom dla kategorii PSIM (Physical Security Information Management) umożliwiając integrację różnych systemów bezpieczeństwa.

Podstawowym urządzeniem systemu jest strefowy kontroler dostępu. Kontroler ten może w oparciu o własne zasoby sprzętowe obsługiwać 2 przejścia dwustronne. Po dołączeniu modułów zewnętrznych, kontroler ten powinien dozorować do 16 przejść dwustronnych. Moduły rozszerzeń są dołączane do kontrolera za pośrednictwem magistrali RS485 z wykorzystaniem protokołu komunikacyjnego. Magistrala musi tworzyć strukturę gwiazdy i mieć długość do 1200 m, licząc od kontrolera do najbardziej odległego modułu. Kontroler musi również współpracować z urządzeniami podłączonymi do sieci komputerowej, który pełni rolę interfejsu komunikacyjnego do urządzeń sieciowych.

Przesyłanie ustawień do kontrolerów jest realizowane w tle i nie zatrzymuje bieżącej pracy systemu. Czas przesyłania ustawień zwykle nie przekracza 1 minuty na każdy tysiąc aktywnych użytkowników systemu. Po zakończeniu przesyłania następuje przełączenie systemu na nowe ustawienia, w trakcie, którego system wstrzymuje pracę na kilka sekund.

System umożliwia zarządzanie użytkownikami w trybie online. W trybie tym, aktualizacja danych użytkownika następuje natychmiast po wykonaniu zmian w bazie danych systemu. Przesyłanie zaktualizowanych danych użytkownika nie zatrzymuje działania systemu i zwykle zajmuje kilka sekund. Zdarzenia zarejestrowane w systemie są na bieżąco pobierane z kontrolerów i zapisywane w bazie danych systemu. Pobieranie zdarzeń następuje automatycznie przez serwer komunikacyjny systemu i nie wymaga działania aplikacji zarządzającej systemem.

W przypadku braku połączenia z serwerem komunikacyjnym, kontrolery zapisują zdarzenia w swoich wewnętrznych buforach pamięci. Zasoby sprzętowe kontrolera dostępu muszą być rozszerzane przez dołączanie zewnętrznych modułów i urządzeń. Zewnętrzne zasoby sprzętowe muszą być wykorzystywane wg tych samych zasad, co zasoby płyty głównej kontrolera. Lokalizacja obiektu (linii wejściowej, linii wyjściowej, czytnika itd.), jak i jego rodzaj (typ linii wejściowej, typ linii wyjściowej, typ czytnika) nie mają wpływu na funkcję logiczną, jaką można powiązać z danym obiektem fizycznym.

2.Dane Techniczne

<u>Kontroler</u>

Kontroler umożliwia obsługę 16 przejść kontrolowanych dwustronnie oraz 32 węzłów automatyki. Koncepcja integracji z systemem alarmowym umożliwia prezentację stanu strefy alarmowej oraz sterowanie jej stanem bezpośrednio z poziomu terminali dostępu. Kontroler udostępnia zaawansowany, a jednocześnie bardzo wydajny sposób zarządzania użytkownikami systemu oraz kształtowania ich uprawnień. Proces konfiguracji kontrolerów systemu jest realizowany współbieżnie, a ilość kontrolerów w systemie nie wpływa na czas jego konfiguracji, który zwykle kończy się przed upływem 1 minuty. Kontroler zarządzany jest z aplikacji narzędziowej, która umożliwia współpracę z serwerową bazą danych Microsoft SQL Server obecnie wykorzystywaną na uczelni. Zarządzanie systemem może być realizowane z poziomu wielu stacji roboczych z programem narzędziowymi przez operatorów o różnym poziomie uprawnień. System udostępnia serwer integracji programowej umożliwiający swobodny dostęp do logu zdarzeń systemu jak i zarządzanie jego użytkownikami. Komunikacja z komputerem zarządzającym jest realizowana za pośrednictwem sieci LAN/WAN z protokołem szyfrowanym

Terminal dostępu

Terminal identyfikacji jest przeznaczony do wykorzystania w systemie kontroli dostępu i automatyki budynkowej. Terminale w muszą umożliwić rozpoznawanie użytkowników za pośrednictwem kart zbliżeniowych standardu 13,56 MHz MIFARE® Ultralight/Classic/DESFire/PLUS, a także za pośrednictwem urządzenia mobilnego (telefonu) wyposażonego w technologię NFC lub Bluetooth oraz kodu PIN.
W przypadku identyfikacji przy wykorzystaniu technologii Bluetooth zasięg odczytu może sięgać do kilku metrów. Pozostałe metody wymagają zbliżenia identyfikatora do czytnika na odległość kilku centymetrów. Identyfikacja mobilna wymaga zainstalowania w telefonie aplikacji dla systemu iOS oraz Android.
Czytnik ma być wyposażony w klawiaturę lub w dwa klawisze funkcyjne oznaczone symbolami, które alternatywnie mogą być wykorzystane do innych celów niż wskazują powiązane z nimi symbole. Terminal musi posiadać interfejs RS485 za pośrednictwem, którego jest podłączany do magistrali komunikacyjnej kontrolera.

Bezpieczeństwo w systemie

System ma oferować wysoki, wielopoziomowy system bezpieczeństwa, na który składają się:

- Zastosowanie kart standardu MIFARE® z programowalnym numerem zapisanym w szyfrowanych sektorach karty (SSN - Secure Sector Number).
- Obsługa kart MIFARE® DESFire® i MIFARE Plus® oraz technologii mobilnej NFC/BLE (z uwagi na posiadane przez zamawiającego karty)
- Złożone Tryby logowania wymagające użycia kombinacji identyfikatorów (np. karta + PIN).
- Komunikacja w sieci LAN/WAN minimalnie szyfrowana metodą z dynamicznie zmienianym kluczem szyfrującym (CBC).
- Szyfrowana komunikacja z terminalami dostępu i ekspanderami dołączonymi do magistrali RS485, hasło do szyfrowania komunikacji na magistrali RS485. Zakres wartości: 4-16 znaków ASCII.
- Autoryzacja zewnętrzna system umożliwia uzależnienie zgody na dostęp na konkretnym punkcie logowania od decyzji zewnętrznej. Decyzja ta może być wydana przez operatora monitorującego system lub z poziomu dedykowanego do tego celu punktu logowania (czytnika).

Wymagany również jest programator/koder kart- służący do zapisu, odczytu konfiguracji i uprawnień poszczególnych użytkowników (komunikacja/zasilanie usb, diody sygnalizujące)

Kontrola dostępu do pomieszczeń

Głównym zadaniem systemu jest realizacja fizycznej kontroli dostępu do pomieszczeń. System ma być skalowalny i umożliwiać obsługę nieograniczonej ilości przejść. Przejścia muszą być kontrolowane jedno lub dwustronnie. Ilość użytkowników systemu nie jest ograniczona. Ograniczeniu podlega ilość użytkowników na poszczególnych kontrolerach dostępu. System ma przesyłać do kontrolera tylko tych użytkowników, którzy posiadają uprawnienie do wykonania jakiejkolwiek akcji na danym kontrolerze.

Raportowanie czasu obecności

System ma rejestrować zdarzenia związane z ruchem użytkowników na terenie objętym elektroniczną kontrolą dostępu. Rejestr zdarzeń ma być wykorzystany do analizy czasu przebywania użytkowników w poszczególnych częściach dozorowanego obiektu. Program narzędziowy ma umożliwić wyznaczenie czasu przebywania użytkowników w dowolnie zdefiniowanych obszarach systemu (tzw. strefy obecności) i w dowolnym zakresie czasowym. Raportowanie czasu obecności osób może odbywać się przez sumowanie cząstkowych czasów przebywania w określonym obszarze lub jako czas, który upłynął od momentu pierwszego wejścia aż do momentu ostatniego wyjścia z obszaru w ramach tego samego dnia.

Integracja z telewizją przemysłową

W ramach integracji z telewizją przemysłową CCTV system ma udostępniać możliwość pobrania i odtworzenia filmu lub zdjęcia zarejestrowanego przez kamerę skojarzoną z danym typem zdarzenia oraz miejscem jego wystąpienia. Opcjonalnie, film lub zdjęcie pobrane z rejestratora ma zostać zachowane w bazie danych systemu (czas przechowywania uzależniony od zasobów dyskowych). Podgląd z kamer ma odbywać się w osobnym oknie programu zadokowanym na dodatkowym monitorze. Okno z podglądem kamery ma się automatycznie przełączać na tą kamerę, która jest skojarzona z ostatnio

zarejestrowanym zdarzeniem. W programie narzędziowym ma zostać zintegrowana obsługa rejestratorów CCTV oraz kamer zgodnych ze standardem ONVIF.

Awaryjne sterowanie przejściem

System ma umożliwiać zarówno otwarcie jak i zablokowanie dowolnej grupy przejść w trybie awaryjnym. Tryb ten ma mieć najwyższy priorytet i nie może być zmieniony przez żaden inny dostępny w systemie mechanizm za wyjątkiem dedykowanej do tego celu funkcji kasującej tryb awaryjny. Sterowanie trybem awaryjnym przejścia musi być realizowane zarówno lokalnie z poziomu urządzeń systemu, jaki i zdalnie z programu narzędziowego.

Rejestracja zdarzeń

Zdarzenia, które wystąpiły w systemie mają być na bieżąco ściągane z kontrolerów i zapisywane w bazie danych systemu. Proces ściągania ma być realizowany przez Serwer komunikacyjny, który jest usługą systemu operacyjnego i nie wymaga uruchomienia programu narzędziowego zarządzającego systemem. W przypadku, gdy połączenie z kontrolerem jest nieosiągalne, zdarzenia są rejestrowane w wewnętrznym buforze zdarzeń kontrolera i są pobierane automatycznie po przywróceniu komunikacji.

Powiadamianie o wystąpieniu zdarzenia

Wystąpienie dowolnego zdarzenia ma automatycznie uruchamiać akcję powiadomienia. Powiadomienie ma odbywać się przez wyświetlenie komunikatu na ekranie monitora, wysłanie wiadomości email lub wysłanie pakietów danych przy pomocy protokołu TCP pod zdefiniowany adres sieciowy. Korzystając z uniwersalnego mechanizmu filtru zdarzeń ma określić dodatkowe warunki (m.in. czas i miejsce wystąpienia zdarzenia), które muszą wystąpić, aby system wykonał powiadomienie. Powiadamianie protokołem TCP ma być użyte to integracji programowej z innymi rodzajami programów w tym z systemem do zarządzania wideo VMS (Wideo Management System) czy także innymi np. BMS (Building Management System) opisanymi w dziale „Integracja”

Monitorowanie zdarzeń

Zdarzenia, które wystąpiły w systemie mają być na bieżąco wyświetlane w oknach Monitorowania online. Każde z okien ma być skonfigurowane do wyświetlania wybranej grupy zdarzeń i dokowane na dodatkowych monitorach.

Monitorowanie obecności

System ma posiadać monitorowanie osób zalogowanych w dowolnie zdefiniowanych obszarach systemu. Musi posiadać możliwość monitorowania wielu obszarów jednocześnie. W szczególnym przypadku monitor obecności ma być użyty w celu prezentacji listy osób, które zarejestrowały się na wybranym punkcie dostępu w następstwie ogłoszenia ewakuacji budynku.

Monitorowanie przejść

System może umożliwiać monitorowanie wybranych przejść i podgląd zdarzeń, które na nich wystąpiły. W momencie wystąpienia zdarzenia system ma możliwość automatycznego wyświetlania podgląd z kamery CCTV skojarzonej z miejscem wystąpienia zdarzenia lub zdjęcie osoby, która została zarejestrowana na tym miejscu.

Mapy

System ma definiować Mapy bazujące na dowolnych podkładach graficznych i nanosić na nie w procesie konfiguracji symbole reprezentujące wybrane elementy systemu (m.in. Przejścia, Punkty logowania, kamery CCTV). Z poziomu widoku Mapy ma być wywołanie podglądu na żywo z kamery skojarzonej z danym symbolem jak też wykonanie komendy zdalnej.

Harmonogramy

Harmonogramy mają umożliwić uzależnienie działania systemu od konkretnego dnia tygodnia i pory dnia. Harmonogramy mają być wykorzystane przy konfigurowaniu działania wielu funkcji systemu, a w szczególności uprawnień dostępu. Stan harmonogramu ma być prezentowany na linii wyjściowej i umożliwić w ten sposób sprzętowe uzależnienie działania systemu od dnia tygodnia i pory dnia.

Uprawnienia

W systemie wykonanie dowolnej akcji ma być uwarunkowane wymogiem posiadania właściwego Uprawnienia. Uprawnienie ma określać, kiedy i gdzie dana akcja (funkcja) może być wykonana. Uprawnienia mają być przypisywane bezpośrednio do Identyfikatora, Użytkownika lub Grupy użytkowników. Uprawnienia przypisane do Grupy dostępu mają przechodzić automatycznie na wszystkich Użytkowników należących do danej Grupy. Uprawnienia przypisane do Identyfikatora automatycznie przechodzić na Użytkownika, do którego dany Identyfikator należy.

Szczególne cechy jakie system kontroli dostępu ma posiadać:

- możliwość definiowania wielofunkcyjnych linii wejściowych
- możliwość definiowania wielofunkcyjnych linii wyjściowych (z możliwością ustawienia priorytetu dla funkcji)
- możliwość definiowania sposobu modulacji linii wyjściowej
- możliwość zastosowania czytników obsługujących standard BLE, NFC podłączanych do kontrolera po szyfrowanej magistrali RS485
- definiowanie własnych trybów logowania
- logowanie zwykłe, specjalne (długie przyłożenie karty – czas definiowany), podwójne; na jednym punkcie logowania możliwość wywoływania wielu funkcji
- komendy globalne wywoływane: dowolnym zdarzeniem w systemie, komendą ze stacji roboczej,
- autoryzacja zewnętrzna (potwierdzenie tożsamości na ekranie Ochrony)

Integracja

- System kontroli dostępu musi oferować możliwość integracji z przyszłymi platformami VMS, które wykorzystując protokół OPC będą miały możliwość komunikacji z innymi systemami (SKD, SAP, SSWiN, CCTV). Dopuszcza się stosowanie zewnętrznych modułów integracji OPC.
- System SKD musi oferować możliwość integracji z przyszłymi platformami VMS, które muszą współpracować z kilkoma rodzajami interaktywnych zasobów - co oznacza, że użytkownik może nie tylko oglądać i nagrywać kanał, ale także sterować nim z aplikacji.
- System SKD musi oferować możliwość integracji z przyszłymi platformami VMS, które muszą umożliwiać tworzenie interaktywnych przycisków umożliwiających wywoływanie komend CGI, wysyłanie żądań http, resetowanie liczników, generowanie alarmów, uzbrajanie/rozbrajanie systemów alarmowych, wyzwalanie wyjść alarmowych.

3. Wymogi oprogramowania

Podstawowe cechy i funkcjonalności aplikacji:

1. Musi posiadać logowania do aplikacji przy użyciu lokalnie przechowywanych kont użytkowników i haseł lub przy użyciu poświadczeń usługi Active Directory posiadanej przez zamawiającego.

Oprogramowanie musi być oparte na otwartej architekturze umożliwiającej konfigurację i zarządzanie urządzeniami systemu kontroli dostępu pochodzącymi od różnych producentów.
System musi mieć możliwość integracji z różnymi modułami, kontrolerami, czytnikami kart i aplikacjami wchodzącymi w skład systemów innych niż oferowany.
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. Możliwość weryfikacji przyczyny alarmu bez jego potwierdzenia.

Usprawnienia w zakresie konfiguracji:

a) Wsparcie konfiguracji urządzenia za pomocą wstępnie skonfigurowanego szablonu przejść.
b) Automatyczne wykrywanie jednostek z wykorzystaniem portów wykrywania i rodzajów wykrywanych jednostek,

c) Możliwość wymiany jednostek (np. istniejącego kontrolera na nowy) z jednoczesnym przechowaniem dzienników i zdarzeń ze starej jednostki.
d) Możliwość wstępnej konfiguracji systemu przed fizyczną instalacją sprzętu.

Możliwość zbiorczej aktualizacji oprogramowania układowego z aplikacji

4. Współpraca z innymi systemami

System musi współpracować z posiadanym przez Uczelnię systemem OPTiCamp obsługującym wykorzystywane przez Uczelnię karty w standardzie Mifare (stykowe i bezstykowe) oraz zapewniającym bazę aktywnych użytkowników. Współpraca między systemami musi być realizowana w sposób ciągły zapewniający w sposób bezzwłoczny dodanie użytkownika lub aktualizację jego statusu pochodzące z systemu OPTICamp.
System musi posiadać możliwość rozbudowy w przyszłości na cały Kampus POLITECHNIKI LUBELSKIEJ. 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,
c) integracja ALPR 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).

5. Prace budowlane

Projekt musi założyć następujące kwestie:
a) Wymiana klamek na gałki- jednostronnie,
b) przejścia przewodów elektrycznych oraz rur przez stropy i ściany muszą uwzględniać zastosowanie atestowanych zabezpieczeń ogniochronnych zgodnie z obowiązującymi przepisami.
c) Elementy stanowiące zabezpieczenia ppoż. muszą być integralną częścią dostawy systemu, wszystkie instalacje wykonywane w ramach zadania wykonać w sposób szczelny, estetyczny
d) W przypadku braku możliwości poprowadzenia przewodów w istniejących korytach dołożenie koryt, rur w taki sposób by części nowo założone były integralną częścią istniejących

6. Pozostałe wymagania dla wykonawcy

a) Przed rozpoczęciem robót Wykonawca zobowiązany propozycję rozwiązań technicznych do zaakceptowania Zamawiającemu.
b) Harmonogram robót podlega akceptacji i uzgodnieniu z administratorem obiektu.
c) W przypadku etapowania robót każdy z etapów podlega weryfikacji i odbiorowi przez Zamawiającego.
d) Po wykonaniu prac Wykonawca jest zobowiązany przedstawić dokumentację powykonawczą w wersji papierowej i elektronicznej (certyfikaty, aprobaty, uprawnienia, opisy szczegółowe wszystkich zastosowanych sprzętów, instrukcje, plany pięter z naniesionymi przejściami, hasła administracyjne, opisy licencji itp.)

7. Gwarancja

Dostarczony System Kontroli Dostępu musi być objęty co najmniej 2 letnią gwarancją producenta oraz 2 letnią gwarancją na wykonane prace przy SKD
Wykonawca ma zapewnić przeszkolenie wszystkich użytkowników sprawujących kontrolę nad danymi pomieszczeniami dodatkowo musi zostać powołana tzw. infolinia- helpdesk/serwisdesk by w momencie problemu po stronie użytkownika była pomoc ze strony wykonawcy na co najmniej 24 miesiące w określonych przypadkach infolinia oraz pomoc na miejscu. 24 godziny na przyjazd na miejsce oraz 12 telefonicznie kiedy naprawę doraźną może wykonać użytkownik.
Wykonawca jest zobowiązany zapewnić w okresie gwarancji przeglądy serwisowe zgodnie z wymaganiami DTR.

8. Wykonawca

Wymagania :

a) Certyfikat w zakresie stosowania biernych zabezpieczeń przeciw pożarowych (minimum 3 osoby)
b) uprawnienia SEP Eksploatacja i Dozór do 1kV – minimum 5 lat (minimum 3 osoby),
c) uprawnienia budowlane do projektowania i kierowania robotami budowlanymi bez ograniczeń w specjalności instalacyjnej w zakresie sieci, instalacji i urządzeń telekomunikacyjnych – minimum 4 lata (minimum 1 osoba).
d) Świadectwo ukończenia szkolenia proponowanego producenta systemu SKD nie starsze niż 1 rok (minimum 3 osoby)
e) Świadectwo ukończenia kursu pracownika zabezpieczeń technicznych do klasy SA4 (minimum 1 osoba)
f) Dostawca systemu SKD musi udokumentować, integrację z platformą VMS w działających obiektach o podobnym zakresie.

9. Inne

Wymaga się poświadczenia wykonania wizji lokalnej w ustalonej dacie przez Zamawiającego. Wykonanie wizji uzasadnia się koniecznością weryfikacji tras instalacji co może mieć wpływ na późniejszą cenę. Zamawiający nie jest w stanie przedstawić racjonalnie rozmieszczenia elementów układu na budynku

Wykonawca dostarczy stosowne oprogramowanie wraz z licencjami wraz z przeniesieniem praw do używania oprogramowania na zamawiającego oraz odpowiedni sprzęt komputerowy który będzie wykorzystany do instalacji opisywanego w treści oprogramowania.

Czas wykonania prac do 10tygodni od podpisania umowy wraz z przekazaniem pełnej dokumentacji.

Definicja skrótów:

PSIM- Physical Security Information Management
LAN/WAN- Local Area Network/ Wide Area Network
NFC- Near Field Communication
CCTV- Closed Circuit TeleVision
ONVIF- Open Network Video Interface Forum
TCP- Transmission Control Protocol
VMS- Wideo Management System
BMS- Building Management System
SKD- System Kontroli Dostępu
SAP- System Alarmu Pożarowego
SSWiN- System Sygnalizacji Włamania i Napadu
OPC- Open Platform Communications

Załączniki:

Zał. nr 1 Rzuty poziomów z zakreślonymi przejściami do wykonania systemu kontroli dostępu
Zał. nr 2 Zdjęcia