System Elektronicznej Kontroli Dostępu

Zaawansowane zarządzanie dostępem fizycznym do pomieszczeń

System Elektronicznej Kontroli Dostępu (system EKD) powinien umożliwiać sprawne zarządzanie oraz kontrolowanie dostępu do pomieszczeń, stref bezpieczeństwa na terenie Szpitala. Zainstalowane w wyznaczonych miejscach czytniki kart zbliżeniowych mają efektywnie ograniczyć dostęp do wybranych pomieszczeń i/lub stref. Uzyskanie dostępu do pomieszczenia będzie możliwe po prawidłowej identyfikacji spersonalizowanego urządzenia uwierzytelniającego (elektronicznej karty EKD przypisanej do pracownika).
Dedykowane oprogramowanie dla systemu EKD powinien umożliwiać:
- nadawanie lub ograniczanie prawa dostępu dla poszczególnych osób lub grup osób (zdalne programowanie uprawnień przypisanych do kart),
- prowadzenie nadzoru oraz kontrolowanie sytuacji w stanach zagrożenia lub alarmowych poprzez wizualizację zdarzeń na dedykowanym stanowisku oraz komunikację e-mail, sms.
- sporządzanie raportów o określonych kryteriach.

System powinien rejestrować co najmniej następujące zdarzenia:

- utworzenie stref bezpieczeństwa obejmujących poszczególne przejścia objęte kontrolą dostępu oraz urządzeń aktywnych (czytniki i urządzenia sterujące),
- wprowadzenia tożsamości użytkownika (wprowadzenia danych osobowych użytkownika do systemu),
- aktywacja urządzenia uwierzytelniającego (aktywacja karty EKD przez administratora systemu),
- przyporządkowanie urządzenia uwierzytelniającego do użytkownika (przypisanie karty EKD do użytkownika)
- zmiana statusu urządzenia uwierzytelniającego (aktywacja, blokada karty EKD),
- zapis zdarzeń w systemie (np. użycie karty EKD, otwarcie drzwi po uwierzytelnieniu, brak otwarcia drzwi po uwierzytelnieniu, włamanie),
- zapis danych w systemie (np. wydanie, zdanie klucza z punktu pobrań wraz z weryfikacją uprawnienia do pobrania)

System powinien posiadać moduł (opcjonalnie) lub współpracować z dedykowanym modułem Rejestracji Czasu Pracy (RCP) bez konieczności dodatkowej integracji.

Elementy systemu EKD

System EKD powinien być zarządzany przez serwer aplikacyjny z bazą danych. Zarządzanie systemem powinno odbywać się z poziomu stacji roboczej poprzez aplikację klienta lub poprzez przeglądarkę webową. Dostęp do systemu będzie możliwy poprzez zalogowanie do imiennego konta użytkownika.
Czytniki systemu EKD powinny spełniać co najmniej następujące wymagania:

- wykorzystywać technologię zbliżeniową,
- gwarantować wysoki poziom bezpieczeństwa,
- gwarantować niezawodność pracy,
- gwarantować wysoką odporność na zewnętrzne warunki

System powinien funkcjonować w oparciu o technologię kart elektronicznych np.: typu MIFARE. Elektroniczna kontrola dostępu (EKD) powinna funkcjonować w sposób nieprzerwany (identyfikacja karty, uruchomienie przejścia, blokada przejścia) nawet w sytuacji utraty zasilania elektrycznego lub uszkodzenia sieci teleinformatycznej Szpitala. Z chwilą przerwania łączności z serwerem, aktywne urządzenia EKD powinny pracować autonomicznie i rejestrować wszystkie zdarzenia. Otwarcie drzwi po uwierzytelnieniu powinno być możliwe nawet w przypadku utraty komunikacji z serwerem oraz braku zasilania głównego. Z chwilą przywrócenia łączności z serwerem, zarejestrowane zdarzenia w urządzeniach aktywnych (np. otwarcie drzwi po użyciu karty EKD) powinny zostać przesłane automatycznie do serwera.

Funkcjonalności systemu

System EKD musi również umożliwiać:

- zdalne zarządzanie uprawnieniami użytkownika tzn. możliwość zmiany uprawnień przypisanych do karty bez konieczności przeprogramowania karty (np. blokada karty w przypadku jej zagubienia, zmiana uprawnień pracownika),
- wykorzystanie kart hybrydowych,
- wykorzystanie tokenów,

Do sterowania systemu EKD dopuszcza się wykorzystanie kart hybrydowych typu smartcard. Układ zbliżeniowy karty zostanie wykorzystany w systemie EKD. Zbliżenie karty do czytnika umożliwi odczyt karty oraz aktywację przejścia w zależności od posiadanych przez właściciela karty uprawnień.
Wysoki poziom bezpieczeństwa zapewniony zostanie poprzez:

- Zapewnienie odporności na tzw. „otwarcie drzwi poprzez zwarcie" czyli demontaż czytnika i wysterowanie zamka drzwi poprzez zwarcie przewodów,
- Użycie kart, których nie będzie możliwe wykonanie duplikatu lub ich sklonowania przez osoby niepowołane
- Dostęp do aplikacji systemu powinien wymagać logowania poprzez podanie indywidualnego loginu użytkownika oraz uwierzytelnienia za pomocą hasła.

System powinien umożliwiać rejestrowanie wydania/zdania klucza na portierni. Dodatkowo system będzie wymagał użycia karty użytkownika by sprawdzić czy użytkownik posiada uprawnienia do pobrania kluczy. Każda czynność powinna zostać zarejestrowana w systemie (wydanie/zdanie klucza, odmowa wydania). System powinien umożliwiać zastosowanie tokenów -- przypinanych do kluczy. Rozwiązanie tego typu umożliwi realizację polityki kluczy oraz zdalne zarzadzanie przywilejami pracowników w tym zakresie. W odniesieniu do pomieszczeń o podwyższonych rygorach bezpieczeństwa zastosowane zostanie rozwiązanie „karta - bezstykowy czytnik kart".

Planuje się uruchomienie funkcjonalności systemu EKD umożliwiającej przełączenie wybranych punktów kontroli dostępu pomiędzy dwoma trybami pracy:

- normalnie otwarty - wówczas możliwe jest wejście do pomieszczenia bez użycia karty (np. gabinet w poradni)
- normalnie zamknięty – wówczas w celu otwarcia drzwi niezbędne jest użycie karty (w przypadku otwarcia drzwi bez użycia karty zostanie wygenerowany sygnał alarmowy włamania).

System EKD powinien umożliwiać nie tylko rejestrację zdarzeń alarmowych (włamanie pojawienie się nieupoważnionej osoby w strefie) ale również wizualizację i powiadomienie odpowiedzialnych za ochronę obiektu służb.

System powinien posiadać funkcjonalności do zarządzania dostępem do dźwigów osobowych.

Wdrożony system EKD będzie funkcjonalnie i infrastrukturalnie zintegrowany z innymi systemami. Bazą komunikacyjną stanie się rozbudowana sieć LAN oraz infrastruktura dostępowa w ramach tej sieci. Bardzo ważnym elementem rozbudowy systemu EKD będzie integracja systemu EKD z systemem Zarzadzania Tożsamością.

System musi spełniać wymagania określone w przepisach prawa w szczególności zasady dotyczące ochrony danych osobowych.