załącznik nr 2

WYTYCZNE DOTYCZĄCE ZABEZPIECZENIA TECHNICZNEGO

Wszystkie rozwiązania systemu kontroli dostępu (SKD) muszą być uzgodnione z rzeczoznawcą ds. zabezpieczeń przeciwpożarowych a wprowadzone rozwiązania nie mogą utrudniać ewakuacji osób i mienia.

Zastosowany system powinien być zgodny z zaleceniami normy PN-EN 60839-11-1 *Systemy alarmowe i elektroniczne systemy zabezpieczeń, część 11-1: Elektroniczne systemy kontroli dostępu, wymagania dotyczące systemów i komponentów.* System kontroli dostępu jako minimalne powinien spełniać wymagania stopnia 2. Zaleca się stosowanie systemu spełniającego wymagania stopnia 3. Wymagania powinny zostać sformułowane w drodze analizy zagrożeń przeprowadzonej dla każdego obiektu.

Wprowadzone i już funkcjonujące w budynkach sądów SKD nie spełniające wymagań, należy dostosowywać uwzględniając te wytyczne w trakcie planowanych lub prowadzonych prac modernizacyjnych.

System musi zawierać możliwość integracji z systemem rejestracji czasu pracy w postaci automatycznego eksportu zdarzeń oraz spełniać wymagania Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych – RODO, w zakresie anonimizacji danych osobowych (zalecana automatyczna anominizacja).

Poniższe wymagania mogą być stosowane jako wytyczne i nie zastępują specyfikacji technicznej, która musi być dostosowana do struktury architektonicznej, organizacyjnej oraz uwarunkowań innych systemów teletechnicznych dla każdego obiektu.

Wymagania techniczne systemu kontroli dostępu.

1. **Interfejs użytkownika.**
    a. ***Tożsamość:***

Podstawowym nośnikiem tożsamości w SKD powinien być identyfikator w postaci karty wykonanej w technologii zapewniającej szyfrowanie informacji na karcie oraz szyfrowaną transmisję z czytnikiem.

W normalnym trybie działania system powinien wykorzystywać do rozpoznania pełną

informację identyfikatora (kod obiektu i numer karty lub niepowtarzalny numer karty).

W awaryjnym trybie pracy system może wykorzystywać do rozpoznania jedynie część informacji identyfikatora (np. tylko kod obiektu).

Numer identyfikacyjny identyfikatora dający się odczytać z identyfikatora nie może być bezpośrednią reprezentacją pełnego kodowania.

W przypadku wykorzystania rozpoznania za pomocą informacji zapamiętanej w połączeniu z identyfikatorem lub biometryką, informacja zapamiętana (kod PIN) wymaga minimum 4 cyfr.

System powinien umożliwiać wykorzystanie czytników biometrycznych. W systemie można stosować wyłącznie czytniki pozwalające na rozpoznanie żywego organizmu. Współczynnik błędnych akceptacji określony na podstawie dokumentacji dostarczonej przez producenta nie powinien być niższy niż 0,3%[1].

b. Wymagania dotyczące rozpoznania tożsamości:

System powinien umożliwiać przyznawanie praw dostępu grupie danych identyfikacyjnych i powinien umożliwiać zmianę praw dostępu grupy danych identyfikacyjnych.

c. Czytniki kontroli dostępu powinny spełniać następujące wymagania:

- wykorzystywać protokół Wiegand-37 lub dłuższy do komunikacji,
- odporny na działanie czynników atmosferycznych, minimum IP55,
- częstotliwość pracy 13,56MHz,
- kodowana transmisja danych pomiędzy czytnikiem i kartą, klucz kodowania 64 bit,
- audiowizualna sygnalizację stanu drzwi (buzzer i/lub diody LED).
- zabezpieczenie przed odwrotną polaryzacją styków zasilających.

2. Kontroler, Interfejs przejścia kontrolowanego.

SKD powinien mieć wyjścia zdolne do sterowania elektromagnesów drzwiowych, zaczepów elektrycznych, aktywatorów montowanych w ościeżnicy, rygli sterowanych elektrycznie, hydraulicznie albo pneumatycznie i/lub innych typów zamków elektromechanicznych oraz elektrycznych dźwigni przeciwpanicznych.

System powinien umożliwić dostęp przyznany warunkowo zależnie od stanu danych identyfikacyjnych (zablokowany, zawieszony, unieważniony).

Kontrolery (sterowniki) współpracujące z czytnikami danych oraz pozostałymi elementami (zamki elektryczne, zwory, rygle, szlabany, triody, bramki, przyciski, czujniki stanu drzwi itp.) powinny posiadać możliwość pracy w trybie sieciowym (ON-LINE) i autonomicznym (OFF-

[1] Zasadność wykorzystania biometryki w SKD należy do decyzji każdego administratora budynku, jednak w obecnej chwili wskazane jest, aby systemy były przygotowane na taką ewentualność, na poziomie zapewniającym odpowiednie bezpieczeństwo przechowywanym danym biometrycznym.

LINE - samodzielna praca kontrolerów SKD tj. bez komunikacji z serwerem, w oparciu o posiadane dane konfiguracyjne w pełnym zakresie funkcjonalnym, buforowanie i rejestracja w pamięci nieulotnej zdarzeń do momentu odzyskania komunikacji z serwerem - wielkość bufora, co najmniej 16000 zdarzeń w każdym sterowniku[2]. Praca w trybie autonomicznym każdego kontrolera (sterownika) powinna zapewniać zachowanie w pamięci nieulotnej uprawnień w zakresie dostępu dla użytkowników, oraz pozostałych parametrów związanych z działaniem kontrolowanego przejścia.

Każdy kontroler winien być wyposażony w dualną pamięć umożliwiającą wykonanie synchronizacji danych kontrolera z serwerem bez konieczności blokowania urządzań SKD (drzwi, kołowrotów, szlabanów) i użytkowników. Jeden kontroler (sterownik) powinien obsługiwać maksymalnie 1 przejście np. drzwi, tripod, bramkę, szlaban bez względu na to czy jest to przejście jedno- (jeden czytnik) czy dwustronnie kontrolowane (dwa czytniki).

Obudowa kontrolera (sterownika) powinna uniemożliwiać bezpośredni dostęp osobom nieuprawnionym. Kontroler winien posiadać możliwość wyposażenia go w dodatkowe wejścia/ wyjścia cyfrowe umożliwiające współpracę z innymi elementami. SKD powinien zapewniać realizacji funkcji antypassback. Obszary kontrolowane, dla których włączona będzie funkcja antypassback muszą posiadać zdefiniowane czytniki wyjścia. Użytkownicy opuszczający obszar kontrolowany mają obowiązek użycia karty. Ponowne wejście do obszaru kontrolowanego bez uprzedniego zarejestrowania wyjścia nie będzie możliwe.

3. **Konsola obsługi.**

   a. ***Wymagania w zakresie sygnalizacji i powiadamiania:***

- sygnalizacja wizualna i/lub dźwiękowa stanu zaryglowania przejścia, aż do chwili przyznania dostępu,
- powiadamianie wizualne, gdy jest przyznany dostęp,
- rejestracja zdarzeń, gdy jest przyznany dostęp,
- powiadamianie wizualne, ostrzeganie i rejestracja zdarzeń, gdy odmowa dostępu nastąpiła w wyniku próby użycia przedawnionego identyfikatora,
- powiadamianie wizualne, ostrzeganie i rejestracja zdarzeń w przypadku odmowy dostępu w wyniku konfigurowalnej liczby prób użycia uprawnionego identyfikatora z nieuprawnioną informacją zapamiętaną,

[2] Liczba zdarzeń bufora w przypadku utraty połączenia z serwerem, powinna być dostosowana do możliwości reakcji na awarie w SKD. Im dłuższy przewidywany czas reakcji i więcej zdarzeń (przejść) tym bufor powinien być większy. Zaproponowane 16000 jest rozwiązaniem dla budynków o dużym nasileniu ruchu i możliwościach reagowania na awarię w przeciągu 24 godzin od wystąpienia.

- możliwość śledzenia karty (wyświetlanie, rejestracja),
- możliwość śledzenia czytnika (wyświetlanie, rejestracja),

Wszystkie zmiany inicjowane przez operatora powinny być rejestrowane z uwzględnieniem: typu, ID operatora, czasu i daty wystąpienia.

b. Program nadzorczy systemu kontroli dostępu powinien zapewniać:

- możliwość ograniczania praw dostępowych – okres ważności karty,
- możliwość podglądu ruchu osobowego na wybranych przejściach w trybie on-line, dla wybranych typów zdarzeń (alarmowych) oraz przejść,
- współpracować ze skanerem dowodów osobistych i paszportów, dla kart gości,
- umożliwiać definiowanie kart dla gości, kart jednodniowych, kart okresowych,
- umożliwiać generowanie raportów ewakuacyjnych z uwzględnieniem ostatniej lokalizacji wszystkich pracowników i zarejestrowanych gości, obecnych na terenie budynku sądu,
- umożliwiać integrację z systemem depozytorów kluczy.

4. Wymagania dotyczące zasilania

Centrala kontroli dostępu powinna być wyposażona w rezerwowe źródło zasilania zdolne do obsługi centrali i jej akcesoriów w określonych warunkach pełnego obciążenia przez czas min. 2 godzin[3]. Warunki obciążenia nie dotyczą konsoli obsługi ani aktywatorów przejścia kontrolowanego.

5. Elementy zabezpieczenia mechanicznego (kołowroty, bramki itp.) powinny spełniać następujące wymagania:

- potwierdzenie pełnego obrotu w SKD,
- wspomaganie przejścia,
- blokada przed ruchem powrotnym,
- przycisk ewakuacyjny z sygnalizacją led potwierdzającą użycie,
- użycie przycisku ewakuacyjnego odnotowane zostaje w SKD,
- drzwi objęte kontrolą dostępu powinny być wyposażone w czujniki kontaktu potwierdzające otwarcie drzwi (np. kontaktrony),

6. Dodatkowe funkcje, które powinien zapewniać system kontroli dostępu:

Pełna otwartość sprzętowa i programowa tj.

- możliwość dodawania kolejnych urządzeń w związku z rozbudową systemu,

[3] Czas pracy w przypadku awarii zasilania należy dostosować do możliwości reakcji na awarię.

- możliwość definiowania, dodawania oraz integracji z innymi urządzeniami związanych z automatyczną identyfikacją,
- możliwość integracji fragmentów systemu w sieciach LAN / WAN tj.
  - jednolite zarządzanie elementami systemu rozmieszczonymi w różnych punktach,
  - możliwość obsługi dowolnej liczby obiektów.
- architektura oprogramowania typu Klient – Serwer,
- zabezpieczenie przed wczytywaniem niezaprogramowanych kart (np. kart płatniczych, urządzeń NFC).

7. Integracja z systemem Rejestracji Czasu Pracy (RCP)

W związku z projektem wdrożenia w sądach systemu RCP w specyfikacji technicznej kontroli dostępu należy uwzględnić fakt, że funkcjonalność systemu RCP w zakresie ewidencjonowania i rozliczania czasu pracy zostanie zaimplementowana do Zintegrowanego Systemu Rachunkowo Kadrowego (ZSRK) a co za tym idzie wymiana danych będzie następowała pomiędzy SKD i ZSRK za pośrednictwem szyny danych.

W celu zapewnienia wymiany odpowiednich danych w specyfikacji technicznej SKD należy uwzględnić poniższe informacje:

a) Minimalne zdarzenia, które system ZSRK będzie mógł przyjmować po wdrożeniu „Rozliczania czasu pracy":

- Rodzaj zdarzenia czasowego:
  - Kod Nazwa (maksymalnie 25 znaków)
  - P10 Wejście
  - P15 Wyjście na przerwę
  - P20 Wyjście
  - P30 Wyjście służbowe

b) SKD nie będzie poddawał danych agregacji.

- Dane powinny zawierać:
  - Kod zdarzenia (słownik: P10, P15, P20, P30),
  - Numer karty (maksymalnie 8 znaków numerycznych np. 00239223),
  - Data zdarzenia (data w formacie RRRRMMDD),
  - Czas zdarzenia (godzina, minuta, sekunda w formacie HHMMSS),

c) Dane z SKD mają być przekazywane w postaci pliku.

- Plik o strukturze jak w punkcie 1,
- plik w formacie .txt lub .csv. Kolumny rozdzielone średnikiem (znakiem średnika „;"),

- kolejne kolumny powinny zawierać informacje:
    - Kod zdarzenia (słownik: P10, P15, P20, P30),
    - Numer karty (maksymalnie 8 znaków numerycznych np. 239223),
    - Data zdarzenia (data w formacie RRRR-MM-DD),
    - Czas zdarzenia (godzina, minuta, sekunda w formacie HH:MM:SS),

d) Udostępnienie bazy danych w SKD, ma się odbywać w formie online za pośrednictwem szyny danych. Zgodnie z wypracowanym zestawem konwencji integracyjnych cała komunikacja w pierwszej kolejności powinna odbywać się w oparciu o WebService'y eksponowane SOAPem 1.1 na chwilę obecną. Komunikacja pomiędzy SKD a szyną powinna następować przez WebService. Pomiędzy szyną danych a ZSRK również przez WebService.

e) SKD powinien dawać możliwość automatycznej wymiany online lub w odstępach czasowych, które można zdefiniować na poziomie sądu. SKD powinien sam inicjować wysłanie danych na szynę danych bez zapytania ze strony ZSRK.

8. Dodatkowe informacje:

- w nowo budowanych systemach kontroli dostępu należy stosować do komunikacji protokół OSDP (np. AES 128.),
- odporność SKD na próby nieautoryzowanego dostępu podnosi zastosowanie dedykowanego klucza kodowania czytników i kart. Rozwiązanie to jednak nie jest racjonalne w przypadku małych sądów, i budynków z małą liczbą przejść, dlatego do rozważenia pozostaje np. wprowadzanie jednolitego rozwiązania w kilku budynkach podległych jednej apelacji,
- w budynkach, w których jest dużo wydawanych kart gości proponuje się wrzutnie kart dla gości opuszczających budynek,
- optymalnym rozwiązaniem przy wdrażaniu SKD jest wykonywanie prac w oparciu o przygotowany projekt, jednakże dokumentacja powykonawcza jest niezbędnym minimum, które należy uzyskać od wykonawcy systemu,
- SKD powinien być naprawiany, konserwowany i poddawany przeglądom technicznym nie rzadziej niż 1 raz w roku. Czynności te powinny być wykonywane przez przedsiębiorców ochrony technicznej oraz pracowników przez nich zatrudnionych posiadających legitymacje kwalifikowanego pracownika zabezpieczenia technicznego oraz świadectwa ukończenia kursów w zakresie instalowania i konserwacji lub projektowania systemów alarmowych.

– Po zainstalowaniu SKD, należy uzyskać od podmiotu instalującego system deklarację zgodności z przyjętymi rozwiązaniami.