Wytyczne Ministerstwa Sprawiedliwości dot. Systemów RCP

1. Interfejs użytkownika.

(źródło: pkt 1 dokumentu źródłowego tj. załącznika nr 1 do pisma Ministerstwa Sprawiedliwości BO-III.5004.4.2021 dot. wytycznych dotyczących zabezpieczenia technicznego z wyłączeniem podpunktu „c", który dotyczy głowicy czytającej na bramkach dostępowych - kołowrotach)

a. Tożsamość:

Podstawowym nośnikiem tożsamości w RCP-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.

2. Integracja z systemem Rejestracji Czasu Pracy (RCP)

(źródło: pkt 7 dokumentu źródłowego w całości)

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 RCP-SKD i ZSRK za pośrednictwem szyny danych.

W celu zapewnienia wymiany odpowiednich danych w specyfikacji technicznej RCP-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

[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.

- P20 Wyjście
- P30 Wyjście służbowe

b) RCP-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 RCP-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 RCP-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 RCP-SKD a szyną powinna następować przez WebService. Pomiędzy szyną danych a ZSRK również przez WebService.

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

3. Dodatkowe informacje:

(źródło: pkt 8 dokumentu źródłowego w zakresie wspólnych elementów RCP i SKD)

– w nowo budowanych systemach kontroli dostępu należy stosować do komunikacji protokół OSDP (np. AES 128.),
– odporność RCP-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,
– optymalnym rozwiązaniem przy wdrażaniu RCP-SKD jest wykonywanie prac w oparciu o przygotowany projekt, jednakże dokumentacja powykonawcza jest niezbędnym minimum, które należy uzyskać od wykonawcy systemu,
– RCP-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.