

## OPIS PRZEDMIOTU ZAMÓWIENIA

**„dostawa i montaż systemu zabezpieczenia wejścia do pomieszczeń w budynku Szkoły za pomocą zamków elektronicznych do drzwi”**

**1. Nazwa obiektu budowlanego:**

Krajowa Szkoła Sądownictwa i Prokuratury

**2. Adres:**

Ul. Przy Rondzie 5, 31-547 Kraków

**3. Inwestor:**

Krajowa Szkoła Sądownictwa i Prokuratury

Ul. Przy Rondzie 5 31-547 Kraków

**4. Kod CPV**

44521120-5 - Elektroniczne zamki bezpieczeństwa

## 1. Opis ogólny zamówienia

### 1.1. Cel zamówienia

Modernizacja dostępu do pomieszczeń administracyjnych oraz sal wykładowych w Krajowej Szkole Sądownictwa i Prokuratury.

### 1.2. Zakres przedmiotu zamówienia:

- 1.2.1. Dostawa i montaż 82 kompletnych zamków dostępowych we wskazanych pomieszczeniach KSSiP
- 1.2.2. Uruchomienie systemu sterowania i nadzoru dostępu
- 1.2.3. Przeszkolenie pracowników w zakresie obsługi, serwisu i konserwacji
- 1.2.4. prace i czynności nie wymienione ale konieczne do wykonania, uruchomienia zamków oraz oprogramowania do ich obsługi

## 2. Wymagania dotyczące zamków i ich obsługi

- 2.1. Zamek w postaci kasety, mocowany zamiast klamki na istniejących drzwiach, z jednoczesnym pozostawieniem dolnej wkładki na klucz, umożliwiającym awaryjne otwarcie drzwi istniejącymi kluczami.
- 2.2. Kontrola dostępu realizowana poprzez elektromechaniczną kontrolę klamki zewnętrznej. Klamka w standardowym trybie pracy pozostaje luźna, użycie klamki i możliwość otwarcia drzwi następuje w momencie autoryzacji karty/PIN'u na czytniku kart
- 2.3. Zamek zasilany bateryjnie – bez dodatkowych instalacji elektrycznych czas pracy min 12 miesięcy
- 2.4. Zamek otwierany kartą zbliżeniową, kodem pin lub kluczem systemowym z wykorzystaniem istniejących wkładek i kluczy
- 2.5. Możliwość integracji systemu z istniejącym systemem dostępowym w KSSiP, opartym na karcie zbliżeniowej nie kodowanej Mifare Classic 4k 13.56 Mhz - Czytnik kart działający w standardzie 13,56 MHz. Kompatybilność z kartami/ tagami/ brelokami w technologii Mifare Classic 1K/4K, DESFire EV1, HID iCLASS SE, SKI Data.
- 2.6. Okucie elektroniczne umożliwia obsługę następujących trybów pracy:
  - 2.6.1. otwarte przejście (tryb office, drzwi otwarte na stałe)
    - 2.6.1.1. za pomocą karty z funkcją office
    - 2.6.1.2. za pomocą komunikatu radiowego z poziomu oprogramowania (system wireless online)
  - 2.6.2. pierwszy użytkownik (drzwi otwarte na stałe przez pierwszego autoryzowanego użytkownika)
  - 2.6.3. standardowy dostęp
  - 2.6.4. tryb podwójnej identyfikacji
  - 2.6.5. PIN (opcjonalnie: w wersji z klawiaturą PIN)
  - 2.6.6. karta + PIN (brak rejestracji użycia PIN'u na karcie)

- 2.6.7. PIN + Karta (rejestracja użycia PIN'u na karcie)
- 2.6.8. tryb blokady (zablokowanie przejścia dla aktualnie uprawnionych użytkowników)
  - 2.6.8.1. możliwość aktywacji za pomocą karty blokującej
  - 2.6.8.2. możliwość aktywacji za pomocą komunikatu radiowego z poziomu oprogramowania (system wireless online)
- 2.7. Kontrola dostępu do pomieszczeń dowolnego przeznaczenia – np. pomieszczeń technicznych, gospodarczych, biurowych itd.
- 2.8. Certyfikacja CE, EN18273, EN1634, IP54
- 2.9. Możliwość podłączenia dodatkowych przewodów bezpośrednio do modułu elektronicznego okucia pozwalających na:
  - 2.9.1. otwarcie przy wykorzystaniu przycisku wyjścia (funkcja request-to-exit)
  - 2.9.2. doprowadzenie sygnału z zewnętrznego kontaktronu magnetycznego (informacja o położeniu stanu drzwi)
- 2.10. Możliwość stosowania w drzwiach o odporności ogniowej (EI90).
- 2.11. Możliwość stosowania w drzwiach o szerokości od 35 do 110 mm.
- 2.12. Okucie pozwala na bezprzewodowe zabezpieczenie dowolnego typu drzwi: drewnianych, stalowych, aluminiowych (wąskoprofilowych) i szklanych:
  - 2.12.1. montaż na istniejącym zamku wpuszczanym w standardzie europejskim (EURO DIN),
- 2.13. Okucie elektromechaniczne wyposażone w moduł pamięci:
  - 2.13.1. pamięć nieulotna
  - 2.13.2. moduł pamięci znajduje się po wewnętrznej, bezpiecznej stronie okucia
  - 2.13.3. 1500 użytkowników i 1000 ostatnich zdarzeń
  - 2.13.4. zegar i kalendarz (czas leni/zimowy)
  - 2.13.5. możliwość aktualizacji uprawnień za pomocą kart zbliżeniowych użytkowników lub komunikatów radiowych w trybie wireless online (automatyczna synchronizacja uprawnień w interwałach co 10 sekund) z poziomu oprogramowania
  - 2.13.6. możliwość pobrania danych z pamięci zamków za pomocą programatora przenośnego / urządzenia serwisowego USB lub w formie komunikatów radiowych w trybie wireless online (automatyczna synchronizacja zdarzeń w czasie rzeczywistym z opóźnieniem uzależnionym od jakości komunikacji radiowej) z poziomu oprogramowania
  - 2.13.7. alerty o niskim stanie baterii wysyłane drogą radiową w trybie wireless
- 2.14. Zasilanie bateryjne
  - 2.14.1. Baterie standardowe np. 1.5V AAA LR03
  - 2.14.2. Żywotność baterii minimum 12 miesięcy
  - 2.14.3. baterie znajdują się po bezpiecznej części wewnętrznej okucia, wymiana baterii nie wymaga demontażu całego okucia
- 2.15. Czytnik kart wyposażony w dwie diody LED

- 2.15.1. diody informujące o autoryzacji, braku autoryzacji, stanie drzwi (tryb stałego otwarcia, drzwi zablokowane) oraz niskim poziomie stanu baterii
- 2.16. Możliwość zastosowania czytnika z dotykową klawiaturą PIN
  - 2.16.1. trzy poziomy autoryzacji – PIN, karta, karta+PIN
  - 2.16.2. buzzer z sygnałem dźwiękowym
  - 2.16.3. klawiatura podświetlana w trzech kolorach: niebieski, zielony, czerwony
- 2.17. Możliwość zastosowania różnych modeli klamek oraz wykończeń i kolorów
- 2.18. Hub komunikacyjny - umożliwiający radiową komunikację między zamkami elektronicznymi a systemem kontroli dostępu
- 2.19. Oprogramowanie pozwalającą na konfigurację oraz obsługę wszystkich urządzeń systemu
- 2.20. Funkcjonalność oprogramowania
  - 2.20.1. możliwość tworzenia kart z dostępem do wszystkich pomieszczeń lub wybranych pomieszczeń
  - 2.20.2. autoryzacja/anulowanie kart użytkowników wraz z określonym czasem aktywacji i ważności karty do określonej, dowolnej grupy pomieszczeń
  - 2.20.3. grupowanie użytkowników: grupy użytkowników, użytkownicy indywidualni.
  - 2.20.4. identyfikacja użytkowników na podstawie nośników RFID
  - 2.20.5. możliwość rejestracji oraz śledzenia zdarzeń (autoryzacja dostępu, brak autoryzacji, niski poziom baterii, funkcja office, użycie klamki wewnętrznej) zapisanych w pamięci zamków elektronicznych.
  - 2.20.6. specjalne uprawnienia użytkowników: funkcja stałego otwarcia, uprawnienia administracyjne (otwarcie zaryglowanych od wewnątrz drzwi)
  - 2.20.7. funkcja zamknięcia obiektu możliwy do pogrupowania według dowolnego schematu
  - 2.20.8. różne poziomy uprawnień użytkowników systemu: ograniczona funkcjonalność dla różnych pracowników, pełna funkcjonalność dla administratora systemu itd.
  - 2.20.9. możliwość konfiguracji zmian czasu o określonych porach (czas letni/zimowy).
  - 2.20.10. raporty w formie plików .xls
  - 2.20.11. kompatybilność z istniejącymi kartami zbliżeniowymi w technologii Mifare Classic 1K/4K,
  - 2.20.12. komunikacja TCP/IP, struktura serwer-klient.
  - 2.20.13. jeden rodzaj licencji bez ograniczeń ilości stanowisk
  - 2.20.14. możliwość integracji z systemami zewnętrznymi na bazie protokołu SOAP
  - 2.20.15. Możliwość konfiguracji notyfikacji e-mail na wybrane adresy mailowe
- 2.21. Rejestracja wszystkich zdarzeń wygenerowanych przez urządzenia systemu oraz możliwość konfiguracji alertów mailowych wysyłanych bezpośrednio do użytkownika/administratora systemu. ( między innymi: błąd komunikacji radiowej, drzwi pozostawione otwarte, alert aktywowany po 3 nieuprawnionych próbach dostępu w okresie poniżej 60 minut, alert aktywowany po 3

nieuprawnionych próbach dostępu na jednym zamku w okresie poniżej 60 minut, moduł radiowy aktywny, moduł radiowy nieaktywny).

- 2.22. Audyt zdarzeń systemowych – rejestracja wszystkich operacji wykonanych z poziomu oprogramowania z ich oznaczeniem.
- 2.23. Przenośny programator służący do inicjalizowania, aktualizowania oraz zbierania zdarzeń z zamków elektronicznych będący łącznikiem pomiędzy urządzeniami systemu i oprogramowaniem
- 2.24. Programator kart zbliżeniowych służący do zapisu oraz odczytu konfiguracji i uprawnień poszczególnych użytkowników przy użyciu ich kart zbliżeniowych/ breloków/ opasek lub innych nośników RFID w standardzie Mifare Classic, DESFire, SKIDATA, iCLASS SE.
- 2.25. Zdalne zarządzanie dostępem dzięki oprogramowaniu (tryb online) np. generowanie jednorazowego kodu otwarcia, kontrola, identyfikacja i aktualizacja informacji o tym kto może otworzyć dane drzwi. Przegląd stanu bezpieczeństwa obiektu. Przyjazny dla użytkownika interfejs dostępny z każdego standardowego komputera, tabletu lub smartfona.
- 2.26. Możliwość odczytu logów z zamków i ich archiwizacja
- 2.27. Szyfrowane protokoły komunikacyjne 128 bitów AES lub równoważny
- 2.28. Certyfikacje antywłamaniowe RC3
- 2.29. Zastosowanie systemu „Multiroom” – tzn. możliwość korzystania z zamka przez kilka kart:
  - 2.29.1. Każda karta dedykowana do zamka ma możliwość otwarcia i zamknięcia pokoju
  - 2.29.2. Po otwarciu pokoju, zamek zostaje otwarty do momentu jego zamknięcia przez jedną z kart przypisanych do danego pomieszczenia
  - 2.29.3. System minimalizujący możliwość przypadkowego zamknięcia już otwartego pokoju. Tzn. Jeżeli jedna osoba otworzyła pokój jedną z kart dedykowanych, to druga osoba próbująca wejść do pokoju, a nie wiedząca o tym że jest już otwarty, nie miała możliwości jego zamknięcia np. do otwarcia pokoju wystarczy przyłożyć kartę do zamka, a do zamknięcia pokoju należy ją przyłożyć i przytrzymać 2 sekundy, sygnał dźwiękowy informujący że pokój jest otwarty i zapalenie zielonej diody lub inne rozwiązanie
  - 2.29.4. Możliwość otwarcia drzwi od środka bez posiadania karty. Ponowne zamknięcie drzwi nie daje możliwości wejścia do pokoju z zewnątrz bez użycia karty dostępowej