Znak sprawy: ZP-261-53/21

Załącznik nr 1
(do Zaproszenia do złożenia oferty
nr 1 do umowy)

OPIS PRZEDMIOTU ZAMÓWIENIA

„Dostawa, montaż i uruchomienie dwóch systemów rejestracji czasu pracy w Sądzie Okręgowym w Siedlcach i Sądzie Rejonowym w Sokołowie Podlaskim"

1. Przedmiotem zamówienia jest dostawa, montaż i uruchomienie, dwóch systemów rejestracji czasu pracy (dalej RCP). Jeden dla Sądu Okręgowego w Siedlcach, drugi dla Sądu Rejonowego w Sokołowie Podlaskim. System RCP wdrażany będzie w trzech lokalizacjach:
   1) budynek Sądu Okręgowego w Siedlcach przy ul. Sądowej 2, 08-100 Siedlce – I RCP,
   2) budynek Sądu Okręgowego w Siedlcach przy ul. Kazimierzowskiej 31, 08-110 Siedlce – I RCP,
   3) budynek Sądu Rejonowego w Sokołowie Podlaskim przy ul. Ks. Bosco 3 Sądowej 2, 08-300 Sokołów Podlaski – II RCP,

W ww. budynkach nie ma obecnie funkcjonującego sytemu RCP. Budynki znajdują się w Siedlcach i Sokołowie Podlaskim. Budynki w Siedlcach są połączone ze sobą siecią światłowodową. Czytniki rejestracji czasu pracy należy umieścić na parterze każdego z budynków, w okolicach wejścia głównego (dokładna lokalizacja do uzgodnienia z Zamawiającym).

2. Ze względu na planowane w późniejszym terminie połączenie systemu RCP z istniejącymi systemami kontroli dostępu (dalej SKD), system RCP musi być oparty na urządzeniach kompatybilnych z SKD KaDe. Kompatybilność powinna zostać zapewniona w pełnym zakresie, między innymi zarządzania z poziomu aplikacji do obsługi systemu „KaDe PREMIUM PLUS2."
3. Czytniki systemu RCP nie będą zwalniały żadnych elementów instalacji SKD, będą służyły jedynie do ewidencjonowania czasu pracy.
4. Okablowanie systemów RCP: od najbliższego PEL do kontrolera oraz pomiędzy kontrolerem, a czytnikiem należy prowadzić w ścianie, pod tynkiem. Wykończone gładzią bruzdy instalacyjne należy zamalować farbą w kolorze ściany.
5. Oba Systemy RCP powinny być skonfigurowane do zarządzania sieciowego, z czego: po jednym stanowisku – administratora systemu i minimum po dwa stanowiska – użytkownicy systemu (z możliwością zwiększenia ilości poszczególnych stanowisk). Systemy RCP zostanie zainstalowany na posiadanych stacjach roboczych o parametrach:
   - System operacyjny: Windows 10, 64 - bitowy
   - Procesor: Intel(R) Core(TM) i3-8100 CPU 3.60 GHz
   - RAM: 8 GB
6. Po zakończeniu instalacji i uruchomieniu RCP Wykonawca przeszkoli pracowników Zamawiającego z obsługi systemu RCP oraz dostarczy dokumentację powykonawczą (opis architektury systemu, instrukcje dla użytkowników i administratora).
7. Wszystkie rozwiązania muszą być zgodne z wymaganiami ustawy o zapewnieniu dostępu osobom ze szczególnymi potrzebami oraz wymaganiami 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.

8. Wejścia i wyjścia RCP należy oznaczyć w czytelny sposób oraz skonfigurować do współpracy ze Zintegrowanym Systemem Rachunkowości i Kadr (dalej ZSRK).
9. W momencie finalnego wdrożenia szyny komunikacji z systemem ZSRK wymogiem bezwzględnym jest integracja z tą szyną po stronie Wykonawcy w ramach udzielonej gwarancji.
10. W serwerowniach budynków: w Siedlcach przy ul. Sądowej 2 i w Sokołowie Podlaskim przy ul. Ks. Bosco 3 należy zainstalować serwery zarządzające systemem RCP oraz odpowiedzialne za integrację z systemem ZSRK.
11. Zgodnie z wytycznymi opracowanymi przez Ministerstwo Sprawiedliwości, czytniki będą odpowiadały jednemu z czterech rodzajów zdarzeń czasowych:

    Kod Nazwa (maksymalnie 25 znaków)

    - P10 Wejście
    - P15 Wyjście na przerwę
    - P20 Wyjście
    - P30 Wyjście służbowe

    Czytniki zostaną podłączone do kontrolera i za pomocą sieci IT z serwerem zarządzającym. Na serwerze zarządzającym będzie pracowało oprogramowanie RCP/SKD oraz aplikacja odpowiedzialna za komunikację systemu RCP z ZSRK.
12. Ze względu na konieczność integracji systemu RCP z planowanym systemem SKD należy zastosować czytniki i kontrolery zgodne z normą PN-EN 60839-11-1 "Systemy alarmowe i elektroniczne systemy zabezpieczeń - Część 11-1: Elektroniczne systemy kontroli dostępu - Wymagania dotyczące systemów i komponentów" w stopniu 3." Zgodność z normą należy potwierdzić stosowną deklaracją producenta na cały system składający się z elementów sprzętowych oraz oprogramowania będącego centralnym elementem zarządzającym oraz monitorującym działanie systemu.
13. System Rejestracji Czasu Pracy powinien charakteryzować się następującymi funkcjonalnościami:
    1) Ewidencja danych pracowników wraz z numerem pochodzącym z systemu SAP,
    2) Ewidencja dostosowana do struktury organizacyjnej sądu z podziałem na poszczególne komórki organizacyjne,
    3) Przenoszenie danych dotyczących nieobecności oraz danych osobowych z systemu SAP,
    4) Tworzenie własnych kodów nieobecności usprawiedliwionych,
    5) Możliwość określenia odrębnych godzin pracy dla poszczególnych komórek organizacyjnych, jak również indywidualnie dla pracowników,
    6) Możliwość określania godzin nieobecności w związku z kodami nieobecności SAP,
    7) Możliwość definiowania indywidualnych godzin pracy dla pierwszego roboczego dnia tygodnia,
    8) Definiowanie dni wolnych od pracy oraz pracujących sobót,
    9) Odnotowywanie wszystkich planowanych nieobecności,

10) Odnotowywanie pracy zdalnej,

11) Generowanie kart czasu pracy: rocznych oraz miesięcznych,

12) Tworzenie raportów dotyczących czasu pracy, spóźnień itp.

13) Ewidencja pracowników, dla których nie jest ustawiony godzinowy czas pracy,

14) Generowanie „listy ewakuacyjnej",

15) Zestawienie obecności osób przebywających w sądzie dla każdego dnia miesiąca i każdej godziny,

16) Definiowanie różnych okresów rozliczeniowych dla poszczególnych pracowników - asystenci, referendarze, urzędnicy itp.

17) Moduł „Ewakuacja" - wgląd do ilości osób aktualnie przebywających w sądzie (informacja o przypisanym nr pokoju oraz nr telefonu),

18) Odrębne zasilanie poza zasilaniem z sieci komputerowej Poe,

14. Karty RFID maja być kompatybilne z MIFARE® działająca na częstotliwości 13,56 MHz pamięcią 1K (do nadruku).

15. Projektowane czytniki powinny umożliwiać odczyt zaszyfrowanych danych z kart RFID Mifare (częstotliwość 13,56 MHz) z ewentualną możliwością wyłączenia odczytu numerów seryjnych kart (CSN/UID). Zastosowane zabezpieczenia danych w karcie powinny uniemożliwić kopiowanie oraz nieuprawniony odczyt danych z kart. Należy zastosować nieskompromitowaną technologię (np. odczyt aplikacji z kart Mifare z szyfrowaniem).

16. System RCP należy dodatkowo wyposażyć w czytnik i oprogramowanie szyfrujące. Za pomocą tego czytnika osoba odpowiedzialna za zarządzanie kartami i dostępem do stref będzie mogła przygotować karty i je zaszyfrować.

17. Zgodnie z wymogami stopnia 3 normy PN-EN 60839-11-1 komunikacja pomiędzy kontrolerem przejść oraz czytnikiem powinna być szyfrowana. Czytniki po odczycie zaszyfrowanych danych z karty powinny w bezpieczny sposób z szyfrowaniem przesłać dane do kontrolera. Nie należy stosować czytników wykorzystujących do komunikacji popularnego interfejsu Wiegand, który nie gwarantuje zabezpieczenia przesyłanych danych. Komunikacja z czytnikami powinna być ciągle monitorowana. W przypadku utraty łączności z czytnikiem odpowiedni sygnał alarmowy powinien zostać wysłany do centralnego oprogramowania zarządzająco-monitorującego. Dodatkowo czytniki powinny być zabezpieczone antysabotażowo i wysyłać odpowiedni sygnał alarmowy w przypadku demontażu czytnika. Do komunikacji należy stosować protokół OSDP.

18. System RCP powinien mieć strukturę opartą o autonomiczne kontrolery sieciowe podłączone do serwera zarządzającego z wykorzystaniem protokołu TCP/IP. Dla zapewnienia niezawodnej pracy systemu, nawet w przypadku awarii sieci, kontrolery powinny cechować się autonomicznym działaniem. W przypadku utraty komunikacji kontrolera z pozostałą częścią systemu kontroler do którego bezpośrednio podłączone są czytniki oraz elementy peryferyjne powinien umożliwiać obsługę wszystkich kart zdefiniowanych w systemie oraz zapis zdarzeń w wewnętrznej pamięci. Zdarzenia powinny zostać automatycznie przesyłane do serwera po przywróceniu komunikacji tak, aby mieć dostęp do zdarzeń zarejestrowanych w chwili awarii łączności lub przy próbie sabotaży systemu.

19. Oprogramowanie

1) Metoda komunikacji:

System SAP ERP HR - będący docelowym rejestrem danych przesyłanych przez SKD - jest częścią Zintegrowanego Systemu Rachunkowości i Kadr (ZSRK). Wymiana danych ze środowiskiem odbywa się z wykorzystaniem centralnej szyny integracyjnej SAP PO - rozwiązaniem klasy ESB. Stanowi ona jedyna bramę dostępową do systemów ZSRK spoza środowiska. Sposób dostępu do metod sieciowych eksponowanych przez szynę integracyjną jest przedmiotem opracowanych przez zespół ZSRK konwencji implementacyjnych. Najważniejsze aspekty komunikacji z szyną integracyjną środowiska ZSRK:

- Komunikacja odbywa się przy zastosowaniu protokołu komunikacyjnego WebService SOAP 1.1,
- Dane wymieniane przez ZSRK i systemy SKD muszą wykorzystywać bezpieczny kanał sieciowy HTTPS (zabezpieczenie - *TLS >1.2*),
- Uwierzytelnienie klienta odbywa się przy użyciu użytkownika technicznego (*Basic Authentication*) udostępnionego przez Ministerstwo Sprawiedliwości,
- Jedynym dopuszczalnym formatem danych jest XML,
- Szyna integracyjna dostępna jest jedynie na poziomie sieci wewnętrznej Ministerstwa Sprawiedliwości (tzw. Sieć LAN - 10.0.0.0/8) - systemy SKD muszą mieć zapewniony dostęp sieciowy do punktów dostępowych (endpoints) środowiska ZSRK,
- W środowisku ZSRK uruchomione są instancje testowe wszystkich systemów uczestniczących w komunikacji - przed uruchomieniem produkcyjnym możliwe jest przetestowanie komunikacji i działania interfejsu end-to-end.

2) Metody sieciowe i struktura danych:

Interfejs ZSRK-SKD udostępnia dwie podstawowe metody sieciowe:

- Metoda EventRegister

  Metoda wykorzystywana do rejestracji pakietów zdarzeń w ZSRK:

  - metoda asynchroniczna,
  - metoda idempotentna - tzn. wielokrotne przesłanie tych samych danych jest odpowiednio obsługiwane przez system i nie powoduje duplikacji rekordów pod warunkiem zgodności identyfikatorów poszczególnych rekordów pomiędzy wywołaniami metody,
  - struktury danych opisane w pliku **EventRegisterOut.wsdl**, załączonym do niniejszego dokumentu,

Żądanie:

Nazwa	Typ	Krotność	Ograniczenia	Opis
EventRegisterRequest	EventRegisterRequest	1		
Event	Event	1..4000		Dane zdarzenia
EventID	xsd:string	1	pattern="[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}"	Identyfikator rekordu - UUID (zgodny z RFC 4122)
CourtCode	xsd:string	1	pattern="\d{8}"	Identyfikator sądu
EventCode	xsd:string	1	pattern="\w\d\d"	Kod zdarzenia
PersonID	xsd:string	1	pattern="\d{8}"	Identyfikator osoby z SKD
Date	xsd:string	1	pattern="\d{8}"	Data zdarzenia (format YYYYMMDD)
Time	xsd:string	1	pattern="\d{8}"	Czas zdarzenia (format HHMMSS)

- Metoda EventStatus

  Metoda EventStatus ma na celu potwierdzenie przetworzenia przesłanych zdarzeń. SKD będą mogły wykorzystywać tę metodę do potwierdzenia spójności danych pomiędzy wewnętrzna bazą danych systemu z ZSRK. Dla obydwu poniższych metod inicjatorem komunikacji (a więc stroną wysyłającą żądania) będą SKD.

  Metoda wykorzystywana do sprawdzenia statusu przesłanych wcześniej zdarzeń:

  – metoda synchroniczna

  – struktury danych opisane w pliku **EventStatusOut.wsdl**, załączonym do niniejszego dokumentu

Żądanie:

Nazwa	Typ	Krotność	Ograniczenia	Opis
EventStatusRequest	EventStatusRequest			
EventID	xsd:string	1..4000	pattern="[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}"	Identyfikator rekordu - UUID (zgodny z RFC 4122)

Odpowiedź:

Nazwa	Typ	Krotność	Ograniczenia	Opis
EventStatusResponse	EventStatusResponse			
EventStatus	EventStatus	1..4000		Status przetwarzania zdarzenia
EventID	xsd:string	1	pattern="[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}"	Identyfikator rekordu - UUID (zgodny z RFC 4122)
Status	xsd:string	1	enumeration="ok, notFound"	Status rekordu

3) Alternatywne sposoby zasilania danymi.

W przypadku chwilowej niedostępności szyny integracyjnej ZSRK (tymczasowy down-time, problemy z połączeniem sieciowym), dane powinny zostać przekazane po odzyskaniu dostępu do interfejsu przez system SKD. W sytuacjach przedłużonych problemów z połączeniem do rejestru możliwe jest przekazanie danych w postaci plikowej. Procedura awaryjnego przekazania danych:

- Wygenerowanie pliku/plików XML w formacie zgodnym ze strukturą danych przekazywanych metodą WebService (payload niezawierający *SOAP Envelope*) - nazwy plików powinny być w formacie:

  SKD_JGnnnnnnnn_YYYYMMDD_HHMMSS.xml, gdzie:

  - **nnnnnnnn** - kod sądu
  - **YYYYMMDD** - data generacji pliku
  - **HHMMSS** - godzina generacji pliku

- Przysłanie plików w postaci załączników do wiadomości e-mail na adres wyznaczony przez administratorów ZSRK
- Przesyłane w ten sposób pakiety zdarzeń zostaną wprowadzone do systemu ERP HR alternatywną metodą zasilania rejestru zdarzeń
- Po odzyskaniu połączenia do interfejsu ZSRK-SKD poprawność rejestracji danych powinna zostać potwierdzona metodą **EventStatus**

Koncepcja nie sugeruje automatycznej wysyłki plików - jedynie wspomina, że konieczna będzie wysyłka wygenerowanych plików na wyznaczony adres e-mail - administrator SKD może to zrobić ręcznie.

20. Zestawienie głównych elementów systemów:

1) Sąd Okręgowy w Siedlcach:

a) Oprogramowanie (z wieczystą licencją dostępową bez ograniczenia użytkowników) - 1 szt.

b) Czytnik kart - 2 szt.

c) Kontroler - 2 szt.

d) Karty - 50 szt.

2) Sąd Rejonowy w Sokołowie Podlaskim:

a) Oprogramowanie (z wieczystą licencją dostępową bez ograniczenia użytkowników) - 1 szt.

b) Czytnik kart - 1 szt.

c) Kontroler - 1 szt.

d) Karty - 50 szt.

GŁÓWNY SPECJALISTA
d/s inwestycji i remontów
Sądu Okręgowego w Siedlcach
Cezary Ciećko