

Opis Przedmiotu Zamówienia

Badania i rozwój w zakresie wymogów bezpiecznej łączności pomiędzy sensorami oraz centrami operacyjnymi

1. Wstęp

Utworzenie bezpiecznej sieci wymiany danych obserwacyjnych na poziomie EUSST wymaga uwzględnienia istnienia dwóch kanałów komunikacji (pomiędzy sensorami a centrami operacyjnymi, oraz centrami operacyjnymi a bazą danych EUSST).

Przedmiot zamówienia obejmuje zadanie przeprowadzenia badań w zakresie metod i środków niezbędnych do ustanowienia bezpiecznego kanału wymiany danych pomiędzy ośrodkami operacyjnymi a sensorami instytucjonalnymi lub komercyjnymi. Wynikiem niniejszego zamówienia będzie opracowanie zestawu zalecanych praktyk i rozwiązań umożliwiających ustanowienie tych powiązań. Wybrane rozwiązanie zostanie przetestowane w pilotażowym studium przypadku, tj. aktywnym sensorze optycznym.

2. Szczegółowe wymagania

Niniejsze badanie będzie miało na celu przygotowanie do nadchodzącego wdrożenia bezpiecznej sieci pomiędzy sensorami a ośrodkami operacyjnymi na poziomie krajowym, z uwzględnieniem wymagań EUSST.

W ramach prowadzonych badań, Wykonawca przedstawi opis stanu obecnego. Opis obecnie stosowanych systemów, procedur oraz specyfikacje techniczne służące do transferu danych z sensora do CO. Przedstawi informację (klasyfikację) o rodzaju przetwarzanych danych takich jak między innymi system plików, środowisko w jakich są przetwarzane, wykorzystywane oprogramowanie, etc.,

Następnie zostanie dokonana analiza zagrożeń i ryzyk występujących w istniejącym stanie. Kolejnym elementem będzie przeprowadzenie badań, mających na celu eliminację lub mitygację istniejących ryzyk i zagrożeń z uwzględnieniem wymagań technicznych, nietechnicznych oraz formalno – prawnych.

Wymagania techniczne -

- Wskazanie rodzaju oraz sposobu zabezpieczenia infrastruktury fizycznej elementów systemu sieciowego wraz z propozycją ewentualnych zmian,
- Wybór sposobu/sposobów wymiany informacji w systemie wraz z jego uzasadnieniem,
- Wskazanie zakresu zabezpieczenia poszczególnych elementów systemu ze względu na wrażliwość przetwarzanych w nich danych (jawne, poufne, zastrzeżone, tajne, etc.),

- Wskazanie sposobów zachowania spójności oraz integralności gromadzonych i przechowywanych danych,
- Określenie ról oraz zakresów odpowiedzialności użytkowników mających dostęp do poszczególnych komponentów infrastruktury sieciowej w tym osób trzecich oraz metod ich kontroli,
- Wskazanie potencjalnych zagrożeń dot. cyberbezpieczeństwa oraz sposobów reagowania na nie,
- Wskazanie narzędzi do bieżącego monitoringu oraz audytów całego systemu oraz poszczególnych jego komponentów,
- Zbadanie oraz wskazanie rozwiązania zapewniającego ciągłość w dostępności i osiągalności systemu, w tym odporność na awarie fizyczne takie jak np. zaniki zasilania.

Wymagania nietechniczne -

- Dokonanie analizy interesariuszy systemu (użytkownicy i beneficjenci informacji pochodzących z systemu),

Wymagania formalno-prawne -

- Przeprowadzenie analizy zgodnie z normą ISO 27001

Obecnie do przesyłania danych, wykorzystywane są zazwyczaj dostępne protokoły komunikacji internetowej, które pomimo swoich zabezpieczeń, mogą okazać się nieodpowiednie w przypadku informacji niejawnych. Należy mieć również na uwadze fakt, iż wymagania bezpieczeństwa poszczególnych państw członkowskich nie są jednolite. Opracowanie architektury sieci, odpowiedniej do wdrożenia w różnych państwach członkowskich, z możliwością realizacji bezpiecznej komunikacji pomiędzy sensorami, a centrami operacyjnymi, ma zatem kluczowe znaczenie dla ustanowienia bezpiecznej sieci EUSST. Wyniki badań powinny ułatwić zrozumienie złożoności wymogów bezpieczeństwa, które należy analizować pod różnymi kątami.

Wykonawca, w ramach prowadzonych badań, dokona analizy kwestii związanych z cyberbezpieczeństwem, uwzględniając takie elementy jak wybór mediów i łączy transmisyjnych, ich architekturę, sposób kodowania lub szyfrowania danych oraz uwierzytelniania aktorów zaangażowanych w procesie komunikacji. Uwzględnione zostaną warunki geopolityczne ze względu na ogólnosiwiatową sieć sensorów.

Wykonawca zostanie zapoznany z procedurami i wymogami bezpieczeństwa obowiązującymi w Partnerstwie EU SST dotyczącymi przesyłu danych. Wykonanie badań, będzie wymagało szeregu konsultacji i spotkań dwustronnych. Pozwoli to na poznanie wymagań nie tylko na poziomie EU SST, ale również poszczególnych państw, umożliwi to w raporcie końcowym zaproponowanie rozwiązań, zaleceń oraz dobrych praktyk możliwych do zaimplementowania w jednolitej sieci EU SST.

Wynikiem końcowym badania będą wytyczne dotyczące projektowania architektury systemów komunikacji pomiędzy sensorami a centrami operacyjnymi na poziomie państw członkowskich. Zostaną również uwzględnione rekomendacje dotyczące

wszystkich rodzajów sensorów stosowanych w Partnerstwie. Opracowane propozycje, zostaną zaprezentowane w formie praktycznej, uwzględniając bezpieczeństwo wymiany danych, przy użyciu demonstratora aktywnego sensora optycznego.

DO UMOWY

3. Etapy realizacji umowy

Szczegółowy harmonogram jest zdefiniowany w sposób następujący:

Nr ETAPU	OPIS/NAZWA AKTYWNOŚCI
ETAP 1	Zaproszenie i przypisanie kontraktu
ETAP 2	Szczegółowe wyjaśnienie wymagań EUSST dla Wykonawcy
ETAP 3	Dwustronne konsultacje pomiędzy Wykonawcą a Zamawiającym, prace badawcze
ETAP 4	Raport pośredni prac badawczo-rozwojowych zawierający: - opis stanu obecnego; - potencjalne zagrożenia, ograniczenia, ryzyka - dalsze kroki;
ETAP 5	Dwustronne konsultacje pomiędzy Wykonawcą a Zamawiającym, kontynuacja prac badawczo-rozwojowych
ETAP 6	Prezentacja wyników ETAPY 1-5 dotyczące wspólnego zrozumienia wymagań dotyczących łączności dla typów sensorów, prezentacja prac wstępnych.
ETAP 7	Dwustronne konsultacje pomiędzy Wykonawcą a Zamawiającym, kontynuacja prac badawczo-rozwojowych
ETAP 8	Praktyczna demonstracja przykładów bezpiecznej wymiany danych Raport końcowy wyników badań

Czas realizacji poszczególnych etapów zadania zostanie ustalony w ramach złożonej przez wykonawcę oferty.