Załącznik nr 1 do Zapytania ofertowego

Opis Przedmiotu Zamówienia
W związku z realizacją projektu pn. *Autonomiczny system kryptograficzny ze wsparciem dla bezpiecznej dystrybucji kluczy jednorazowych*, współfinansowanym przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Osi Priorytetowej 1 Regionalnego Programu Operacyjnego – Lubuskie 2020, jednym z celów Zamawiającego jest rozwój kadry i zaplecza technicznego w zakresie badań i rozwoju w obszarze cyberbezpieczeństwa. W związku z powyższym, Zamawiający w postępowaniu wyłoni Wykonawcę, od którego zakupi nieopatentowaną wiedzę techniczną w zakresie szyfrowania kluczem jednorazowym, zgodnie z poniższym opisem.
Postanowienia ogólne, dotyczące wszystkich części zamówienia
Wykonawca zobowiązany jest realizować zamówienia zgodnie z wnioskiem o dofinansowanie, w ramach którego ogłoszone zostało niniejsze postępowania oraz dokumentacją konkursową do niego.
Miejsce realizacji usługi: siedziba Zamawiającego i/lub zdalnie.
Kontakt z Zamawiającym będzie się odbywał: ▪ osobiście – w czasie spotkań w siedzibie Zamawiającego w liczbie zadeklarowanej w formularzu ofertowym, przy czym Zamawiający wymaga udziału Wykonawcy w minimum 1 spotkaniu, zgodnie z wyznaczonym przez Zamawiającego terminie. ▪ zdalnie – za pomocą dostępnych mediów elektronicznych, tj. co najmniej wiadomości e-mail, telefonicznie, przy wykorzystaniu funkcjonalności Platformy będącej w posiadaniu Zamawiającego (Wykonawca otrzyma login i hasło do platformy niezwłocznie po podpisaniu umowy. Dostępne funkcjonalności to m.in. forum, chat).
Odbiór prac Wykonawcy następował będzie poprzez podpisanie, przez Zamawiającego, protokołu odbioru prac bez uwag i zastrzeżeń.
Po podpisaniu protokołu odbioru prac bez uwag i zastrzeżeń, Wykonawcy zostanie wypłacone wynagrodzenie na podstawie poprawnie wystawionej faktury VAT.
Przedstawiona przez Wykonawcę oferta będzie zawierała pełną cenę na zakup rozwiązania dedykowanego w zakresie systemu szyfratora z prawem wyłączności i prawem do modyfikacji rozwiązań na bazie opracowania realizowanego w ramach niniejszego zamówienia.
1. Zakup praw do nieopatentowanej wiedzy technicznej w zakresie szyfrowania kluczem jednorazowym
Zadaniem Wykonawcy będzie opracowanie algorytmu pozwalającego na szyfrowanie danych kluczem jednorazowym, zgodnie z założeniami przyjętymi przez Wykonawcę stawianymi przed finalnym produktem IT w postaci autonomicznego urządzenia szyfrującego dane różnymi algorytmami kryptograficznymi z uwzględnieniem możliwości wymiany kluczy. Zamówieniem objęty jest zakup praw do nieopatentowanej wiedzy technicznej w zakresie szyfrowania kluczem jednorazowym. Zamawiający planuje w projekcie osiągnięcie poniższych rezultatów: 1) Autonomiczność systemu szyfrowania z kluczami jednorazowymi;

2) Urządzenie rekonfigurowalne zapewniające dłuższy czas życia produktu i przyjazne ekologii;

3) Uniwersalność urządzenia kryptograficznego umożliwiająca użyteczność w wielu różnych zastosowaniach.

W opracowywanym rozwiązaniu zastosowane zostaną metody szyfrowania asymetrycznego. Dane będą szyfrowane przy wykorzystaniu pary kluczy (klucz publiczny oraz klucz prywatny) – jeden do szyfrowania treści, drugi do jej odszyfrowania. Dane zaszyfrowane przez klucz nie będą możliwe do odszyfrowania tym samym kluczem, a znajomość jednego z kluczy nie da możliwości odgadnięcia drugiego. Proponowane rozwiązanie łączy w sobie funkcje szyfrowanego pendriva z funkcją szyfratora. Prócz możliwości przenoszenia danych na zabezpieczonym flash dysku (poprzez pin, czytnik papilarny, bądź połączenie tych zabezpieczeń), urządzenie da możliwość szyfrowania kluczem prywatnym i generowania klucza publicznego danych znajdujących się na sprzęcie, do którego podłączony jest flash dysk – bez konieczności instalowania na sprzęcie dodatkowych sterowników, czy oprogramowania. W założeniach, po podłączeniu urządzenia pod komputer, tablet, czy smartfon - użytkownik będzie miał możliwość przesyłania, zaszyfrowanych prywatnym kluczem, wiadomości e-mail, bądź sms, będzie miał również możliwość szyfrowania danych znajdujących się w pamięci laptopa, czy telefonu. 3) Planowane wykorzystanie strumienia różnicowego dla zaprogramowania dynamicznego nowej wartości klucza w FPGA jest dotychczas niestosowanym podejściem w realizacji systemów kryptograficznych, w szczególności, gdy rozmiar danych programujących może znacznie przekraczać rozmiar klucza. Przyjmując, że klucz będzie rozmiaru 128 bitów strumień różnicowy dla FPGA może mieć rozmiar kilkadziesiąt, a nawet kilkaset tysięcy bajtów i bez znajomości poprzedniej konfiguracji możliwości odtworzenia topologii połączeń oraz funkcji układu są bardzo trudne lub nie możliwe do odzyskania bez wejścia w posiadanie danego egzemplarza układu. Jest to nowy sposób wykorzystania algorytmu RSA jako rozwiązanie, w którym jeden ze składników klucza publicznego nie jest jawnie publikowany, a jedynie przekazywany jest opis pozwalający na wygenerowanie nowej wartości klucza.

Główna cecha/funkcjonalność rezultatu projektu to autonomiczność systemu szyfrowania z kluczami jednorazowymi. Korzyść: Bezpieczeństwo i przenośność związana z uodpornieniem systemu na cyberataki polegające na wprowadzaniu złośliwego oprogramowania oraz powtórnemu wykorzystaniu danych szyfrujących.

Głównie założenia realizowanego przedsięwzięcia: urządzenie szyfrujące/deszyfrujące spełnia co najmniej poniższe wymogi:

1) Szyfrowanie/deszyfrowanie danych odbywa się na przenośnych pamięciach USB (pendrive) i na dyskach sieciowych.
2) Do szyfrowania i deszyfrowania danych, urządzenie korzysta z kluczy jednorazowych. Przechwycenie wiadomości zaszyfrowanej i odszyfrowanej nie powinno dawać szansy na odszyfrowanie kolejnych wiadomości, jeżeli nie posiada się samego urządzenia.
3) Dla danych do zadanej wielkości (np. 5kB) szyfrowanie odbywa się z wykorzystaniem jednego klucza. Dla danych powyżej zadanej wielkości, pliki do zaszyfrowania są dzielone na mniejsze „paczki” i każda z nich jest szyfrowana innym kluczem. Posiadając jeden z kluczy nie ma wówczas możliwości odszyfrowania całego pliku.

4) Użytkownik musi mieć możliwość wybrania algorytmu szyfrowania. 5) Urządzenie w czasie pracy może być podłączane do zasilania, ale do działania nie powinno być konieczności podłączania go do komputera i sieci Internet (poza trybem szyfrowania danych w sieci lokalnej).
Planowany okres realizacji zamówienia: od podpisania umowy do 31 grudnia 2019 roku zgodnie z harmonogramem ustalonym z Zamawiającym niezwłocznie po podpisaniu umowy.