

Załącznik nr 1 do zapytania ofertowego

Nazwa zadania: Zakup specjalistycznego oprogramowania do szyfrowania poczty i dokumentów w ramach projektu grantowego „Cyfrowa Gmina” o numerze POPC.05.01.00-0001/21-00”

Zamówienie współfinansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020, Oś Priorytetowa V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU, Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia.

Przedmiotem zamówienia jest sprzedaż, dostawa, instalacja oprogramowania w siedzibie Zamawiającego oraz wdrożenie i szkolenie wskazanych przez Zamawiającego pracowników z podstawowych funkcjonalności oprogramowania.

Wymagania dotyczące oprogramowania:

1. Możliwość pracy dla min. 50 użytkowników przez min 4 lata
2. Oprogramowanie ma pozwalać na szyfrowanie poczty e-mail (obsługa klientów web home oraz klientów poczty takich jak MS Outlook oraz Thunderbird)
3. Szyfrowanie nie może wymagać stosowania trudnych kluczy PGP oraz płatnych certyfikatów kwalifikowanych
4. Ma zapewniać zabezpieczenie dostępu do ustawień konfiguracyjnych oprogramowania przez hasło administratora
5. Baza danych hasel generowanych do szyfrowanego maila
6. Baza danych hasel generowanych do szyfrowanego pliku lub katalogu
7. Generator hasel zgodny z normą ISO 27001
8. Integracja z komórką (Android, IOS, Windows Phone) umożliwiającą wygenerowanie sms-a z hasłem i docelowym kontaktem
9. Lista wygenerowanych hasel wraz z lokalizacją zaszyfrowanych plików lub katalogów
10. Możliwość zastosowania procedur potwierdzających odbiór maili zgodnie z KPA (uprawnieni użytkownicy mogą odszyfrować email dopiero po kontakcie z urzędem)
11. Szyfrowanie algorytmem AES256 treści wiadomości, szyfrowanie algorytmem AES256 załączników, szyfrowanie algorytmem AES256 plików, szyfrowanie algorytmem AES256 katalogów,
12. Do odszyfrowania treści wiadomości, plików, katalogów, załączników email nie wymagane jest połączenie Internetowe. Wystarczy aby klient pocztowy raz pobrał wiadomość która potem np może być przesyłana w środowiskach zamkniętych z ograniczonym dostępem do internetu lub przesyłana dalej do serwerów pocztowych służących wyłącznie dla wewnętrznego dostępu i obiegu informacji.
13. Odszyfrowanie treści wiadomości, plików, katalogów, załączników email jest możliwe na popularnych systemach operacyjnych z środowiskiem graficznym: Windows 8.1, Windows 10, Windows 11, Android
14. Ma dawać możliwość generowania bezpiecznego hasła (litery, cyfry, znaki) o określonej minimalnej długości dla szyfrowania,
15. Do odszyfrowania wiadomości nie może być potrzebne wysyłanie linków do oprogramowania deszyfrującego.
16. Ma pozwalać na Kontrolę każdego/wybranego użytkownika aby świadomie stosował lub rezygnował z szyfrowania emaili



17. Odszyfrowanie wiadomości pocztowych ma bezproblemowo działać dla minimum klientów pocztowych (MS Outlook oraz Thunderbird) oraz przeglądarek www (Mozilla Firefox, Opera, Chrome, Microsoft Edge)
18. Kontrola każdego/wybranego użytkownika aby świadomie stosował lub rezygnował z szyfrowania email
19. Szyfrowany email ma uniemożliwiać dostęp osobom niepowołanym po stronie odbiorcy w sytuacji gdy np kilku użytkowników korzysta z 1 adresu email i tego samego klienta pocztowego
20. Odszyfrowanie nie może wymagać od nadawcy wiadomości oraz odbiorcy zaszyfrowanego email specjalistycznej wiedzy ani kosztów. Nie może także wymagać od odbiorcy instalacji jakiegokolwiek oprogramowania
21. Dodatkowo system ma pozwalać na wykrywanie:
 - Fałszywych maili;
 - Próby podszycia się pod dowolnego adresata;
 - Próby wyłudzenia danych np. bankowych;
 - Próby nakłonienia użytkownika do pobrania niebezpiecznego oprogramowania;
 - Fałszywe linki i odsyłacze w wiadomościach mailowych;
 - Wirusy znajdujące się w odsyłanych linkach i dokumentach Office;