Załącznik nr 1 – Specyfikacja Systemu
(Postępowanie nr NBB/W/641/19)

SPECYFIKACJA W ZAKRESIE DOSTARCZANIA:

1. OPROGRAMOWANIA UMOŻLIWIAJĄCEGO SZYFROWANIE POŁĄCZENIA GŁOSOWEGO, TEKSTOWEGO Z MOŻLIWOŚCIĄ PRZESYŁANIA PLIKÓW

a) W założeniu oprogramowanie do realizacji zadań ma wykorzystywać serwer zapewniający poufność i anonimowość informacji.
b) System ma zapewniać anonimowość adresów IP rozmówców na każdym etapie prowadzenia rozmowy głosowej tzn. eliminacja możliwości wskazania rozmówców
c) System powinien umożliwiać całościowe wdrożenie w ramach infrastruktury Zamawiającego
d) System powinien umożliwiać ustawienia blokady liczby użytkowników
e) System powinien gwarantować zabezpieczenie danych aplikacji poprzez ich zaszyfrowanie na danym urządzeniu. Klucz do szyfrowanej bazy danych nie może znajdować się na urządzeniu
f) System powinien zapewniać użycie protokołu ZRTP z protokołami DH
g) System powinien umożliwiać sprawdzenie urządzenia pod kątem aplikacji szpiegujących: na zasadzie sprawdzenia ilości procesów obsługujących urządzenie w zakresie aparatu oraz mikrofonu
h) System powinien dawać możliwość prowadzania tekstowych rozmów grupowych
i) System powinien umożliwiać wprowadzenie alfanumerycznego kodu do aplikacji
j) System powinien umożliwiać wprowadzenie alternatywnego alfanumerycznego kodu do aplikacji powodującego wyzerowanie aplikacji do stanu sprzed instalacji
k) System powinien zapewniać funkcjonalność wymuszenia, po min. 80 minutach ciągłej konwersacji głosowej, wygenerowania nowych kluczy szyfrujących
l) System powinien działać na systemach operacyjnych OIOS oraz Android

2. OPROGRAMOWANIA UMOŻLIWIAJĄCEGO SZYFROWANIE ZASOBÓW INFORMATYCZNYCH, SZYFROWANIE POCZTY ELEKTRONICZNEJ

a) Oprogramowanie ze względu na konieczność zapewnienia bezpieczeństwa danych wrażliwych, powinno być rozwiązaniem bezpiecznym opartym o technologię kryptograficznej ochrony danych, gwarantującej podwyższony poziom ochrony prywatnych kluczy szyfrujących, który realizowany będzie poprzez technologię zapewniającą, że nie będą one przetrzymywane w całości w jednym miejscu.
b) Szyfrowanie danych będzie realizowane na urządzeniu klienckim
c) Oprogramowanie będzie gwarantować, że wszelkie dokumenty zarchiwizowane, które klient umieszcza na serwerze przechowywane są w formie zaszyfrowanej
d) Szyfrowanie end to end – współdzielone pliki powinny być szyfrowane i przekazywane zawsze w postaci zaszyfrowanej
e) Szyfrowanie powinno odbywać się na stacjach roboczych użytkownika
f) Klucz prywatny nie może być przetrzymywany w jednym miejscu (na stacji roboczej lub serwerze) z wyjątkiem momentu generowania klucza na stacji roboczej lub urządzeniu mobilnym.
g) Szyfrowanie kanału przesyłu danych na poziomie równym lub wyższym niż technologia Point to Point Tuneling Protocol