Załącznik Nr 1 – Szczegółowy opis przedmiotu zamówienia

Spis treści:

1. Cel realizacji zamówienia:

Inicjatywa WiFi4EU ma na celu wsparcie działań, które:

1. są realizowane przez gminy, które muszą zaplanować i nadzorować instalację wewnętrznych lub zewnętrznych lokalnych punktów dostępu bezprzewodowego w miejscach publicznych i które muszą zobowiązać się do:
   a) utrzymania w pełni funkcjonalnych sieci WiFi4EU przez okres trzech lat, począwszy od daty zatwierdzenia umowy o udzielenie dotacji;
   b) rekonfiguracji sieci WiFi4EU w celu podłączenia ich do rozwiązania na potrzeby bezpiecznego uwierzytelniania i monitorowania w pełnej zgodności z wymogami określonymi dalej w niniejszym dokumencie.
2. wykorzystują szybkie łącza szerokopasmowe umożliwiające użytkownikom korzystanie z Internetu wysokiej jakości, który:
   a) jest świadczony bezpłatnie i na niedyskryminujących warunkach, jest łatwo dostępny, zabezpieczony i wykorzystuje najnowsze i najlepsze dostępne urządzenia zdolne do zapewnienia użytkownikom łączności o dużej przepustowości;
   b) umożliwia dostęp do innowacyjnych usług cyfrowych, na przykład usług świadczonych za pośrednictwem infrastruktury usług cyfrowych;
   c) w celu zagwarantowania dostępności zapewnia dostęp do usług przynajmniej w odpowiednich językach danego państwa członkowskiego oraz w miarę możliwości, w innych językach urzędowych UE;
   d) jest udostępniany w miejscach lokalnego życia publicznego, w tym w przestrzeniach zewnętrznych dostępnych dla ogółu społeczeństwa w życiu publicznym społeczności lokalnych;

2. Podstawowe wymogi funkcjonalne

Wymogi dotyczące konfiguracji sieci WiFi4EU i podłączenia jej do rozwiązania stosowanego przez KE na potrzeby monitorowania

1. Wykonawca zapewni, aby punkty dostępu finansowane za pomocą bonu WiFi4EU rozgłaszały wyłącznie identyfikator SSID „WiFi4EU" oraz aby obowiązki opłat, reklamy i wykorzystania danych określone dalej w niniejszym dokumencie były w pełni realizowane.
2. Wykonawca zapewni, aby sieć WiFi4EU z identyfikatorem SSID „WiFi4EU" była otwartą siecią w takim sensie, że nie będzie wymagać żadnych informacji uwierzytelniających (takich jak stosowanie hasła). Po tym, jak użytkownik połączy się z siecią, sieć WiFi4EU z identyfikatorem SSID „WiFi4EU" wyświetli portal autoryzacji http przed autoryzacją połączenia użytkownika z Internetem.
3. O ile nie jest to wymagane przez przepisy krajowe zgodnie z prawem unijnym, połączenie z Internetem poprzez identyfikator SSID „WiFi4EU" ma nie wymagać rejestracji ani uwierzytelniania w portalu autoryzacji i ma być realizowane za pomocą przycisku „kliknij, aby połączyć" w portalu autoryzacji.

3. System autoryzacji:

Podłączenie sieci do rozwiązania stosowanego przez KE na potrzeby monitorowania przebiega w dwóch fazach:

- **Faza I**
  a) Do obowiązków każdego beneficjenta należy rejestracja, uwierzytelnianie, autoryzacja i zliczanie użytkowników zgodnie z prawem UE i prawem krajowym.
  b) Beneficjent zapewnia zgodność z następującymi wymogami dotyczącymi portalu autoryzacji SSID „WiFi4EU":
  c) Do interakcji z użytkownikami sieć WiFi4EU z identyfikatorem SSID „WiFi4EU" wykorzystuje portal autoryzacji http.
  d) Portal autoryzacji ustala okres automatycznego rozpoznawania uprzednio połączonych użytkowników, tak aby portal ten nie był ponownie wyświetlany przy ponownym połączeniu. Powyższy okres jest automatycznie resetowany codziennie o godzinie 00:00 lub przynajmniej ustawiony na maksymalnie 12 godzin.
  e) Nazwa domeny powiązana z portalem autoryzacji http musi mieć zwyczajowy zapis (nie IDN) i składać się ze znaków od a do z, cyfr od 0 do 9, łącznika (-).
  f) Identyfikacja wizualna: portal autoryzacji musi zawierać identyfikację wizualną WiFi4EU.
  g) W portalu autoryzacji musi być wbudowany fragment kodu śledzenia (snopek) zapewniający zdalne monitorowanie sieć WiFi4EU. Instrukcja instalacji snippetu dostępna jest pod następującym adresem: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/wifi4eu. Celem fragmentu kodu śledzenia nie jest gromadzenie jakichkolwiek danych osobowych. Służy on do zliczania liczby użytkowników łączących się z siecią WiFi4EU, załadowania identyfikatora wizualnego WiFi4EU i sprawdzania, czy jest on poprawnie wyświetlany.
  h) Portal autoryzacji zawiera zastrzeżenie prawne, w którym wyraźnie informuje się użytkowników o tym, że WiFi4EU jest publiczną siecią otwartą. Zastrzeżenie powinno również zawierać zalecenia dotyczące środków ostrożności, które są zwykle przekazywane w przypadku dostępu do Internetu za pośrednictwem takich sieci.

i) Beneficjent ma prawo do tworzenia odrębnych sieci WiFi4EU finansowanych tym samym bonem, mających inne nazwy domeny i inne portale autoryzacji.

Faza I trwa do momentu otrzymania przez beneficjenta powiadomienia, że została uruchomiona faza II. Po otrzymaniu wspomnianego powiadomienia beneficjent będzie zobowiązany – na podstawie art. 9 umowy o udzielenie dotacji – do zmiany konfiguracji sieci zgodnie z wymogami doprecyzowanymi w powiadomieniu, w terminie wskazanym w powiadomieniu.

- **Faza II**

Na późniejszym etapie na szczeblu UE opracowany zostanie system bezpiecznego uwierzytelniania i monitorowania, który będzie mógł ewoluować w stronę sfederowanej architektury. Oczekuje się, iż rozwiązanie na potrzeby bezpiecznego uwierzytelniania i monitorowania zostanie wdrożone w roku 2020; Na podstawie art.9 umowy o udzielenie dotacji, po uruchomieniu rozwiązania na potrzeby bezpiecznego uwierzytelniania i monitorowania, beneficjent zmienia konfigurację swoich sieci WiFi4EU w celu podłączenia ich do tego systemu. Ta rekonfiguracja będzie obejmować utrzymywanie otwartego identyfikatora SSID „WiFi4EU" za pomocą portalu autoryzacji, poprzez dodanie identyfikatora SSID „WiFi4EU" dla odpowiednio zabezpieczonych połączeń (poprzez zmianę istniejącego zabezpieczonego systemu lokalnego na system wspólny lub po prostu poprzez dodanie trzeciego identyfikatora SSID) oraz zapewnienie, aby przedmiotowe rozwiązanie mogło monitorować sieci WiFi4EU na poziomie punktów dostępu.

Rejestracja i uwierzytelnianie użytkowników w ramach otwartego identyfikatora SSID „WiFi4EU" oraz lokalnych SSID dla zabezpieczonych połączeń, o ile takie istnieją, a także autoryzacja i zliczanie użytkownikowi w odniesieniu do wszystkich SSID pozostaje odpowiedzialnością każdego beneficjenta zgodnie z prawem UE i prawem krajowym.

4. Podstawowe wymogi techniczne dotyczące urządzeń Wi-Fi w ramach sieci WiFi4EU

Wykonawca zapewni następujące możliwości w przypadku każdego punku dostępu:

a) obsługa współbieżnego wykorzystania dwóch pasm (2,4 GHz – 5 GHz);
b) cykl wsparcia powyżej 5 lat;
c) średni czas pomiędzy awariami (MTBF) wynoszący co najmniej 5 lat;
d) posiadanie specjalnego i scentralizowanego pojedynczego punktu zarzadzania dla wszystkich punktów dostępu w ramach każdej sieci WiFi4EU;
e) obsługa IEEE 802.1x;
f) zgodność ze standardem IEEE 802.11ac Wave I;
g) obsługa IEEE 802.11r;
h) obsługa IEEE 802.11k;
i) obsługa IEEE 802.11v;
j) możliwość obsługi co najmniej 50 użytkowników jednocześnie bez pogorszenia funkcjonowania;
k) posiadanie co najmniej 2x2 nadajników i odbiorników (system wieloantenowy MIMO);
l) zgodność z programem Hotspot 2.0 (program certyfikacji Passpoint organizacji Wi-Fi Alliance).

W celu zapewnienia użytkownikom wysokiej jakości usług za pośrednictwem finansowanej sieci WiFi4EU Zamawiający musi wykupić abonament na połączenie zapewniające prędkość pobierania danych wynoszącą co najmniej 30 Mb/s. Zamawiający zapewni również, aby prędkość tego łącza dosyłowego była co najmniej równa

prędkości łącza (o ile takowe istnieje), które jest wykorzystywane przez Zamawiającego na potrzeby wewnętrznej łączności.

5. Obowiązki dotyczące opłat, reklamy i wykorzystania danych

a) Zamawiający zapewni użytkownikom końcowym bezpłatny dostęp do sieci WiFi4EU, tj. bez odnośnego wynagrodzenia w postaci bezpośrednich płatności czy też innego rodzaju świadczeń, a w szczególności bez konieczności oglądania reklam handlowych lub udostępniania danych osobowych w celach komercyjnych.

b) Zamawiający gwarantuje, że dostęp użytkowników końcowych za pośrednictwem operatorów sieci łączności elektronicznej jest również świadczony w sposób niedyskryminujący, tj. bez uszczerbku dla ograniczeń wymaganych na mocy prawa Unii lub prawa krajowego zgodnego z prawem Unii, z zastrzeżeniem konieczności zapewnienia sprawnego funkcjonowania sieci, w szczególności konieczności zapewnienia sprawiedliwej alokacji zdolności przepustowej miedzy użytkownikami w okresach szczytowych.

c) Regularne przetwarzanie danych do celów statystycznych i analitycznych jest możliwe na potrzeby promowania, monitorowania lub poprawy działania sieci. W tym celu przechowywane lub przetwarzane dane osobowe należy odpowiednio zanonimizować zgodnie z odpowiednimi informacjami o polityce prywatności właściwymi dla danej usługi.

6. Wymagania dodatkowe (techniczne)

a) Wymiana/montaż kabli typu Ethernet kat. 6 (zewnętrznych) między przełącznikiem a AP wg. specyfikacji:
   - Budynek PWSZ – kier. Skwer: 15m + maszt
   - Budynek PWSZ – kier. Parking: 25m
   - Wieżowiec Moniuszki 4: 10m
   - Budynek KDK: 20m
   - Budynek po CIM: 10m + maszt
   - Słupek (Bulwar): 5m
   - Budynek UM – kier. Bulwar: 10m
   - Budynek UM – kier. Pl. Wolności: 10m
   - Budynek - Żłobek: 20m + maszt
   - Budynek na Pl. Zamkowym: 3m

b) Zewnętrzne punkty dostępowe wyposażone w port PoE-out (Power over Ethernet),

c) Wykonawca wyposaży każdy punku dostępu w zasilacz Power over Ethernet zgodny z rekomendacją producenta.

d) Możliwość bezpośredniego podłączenia kamery zgodnej z normą 802.3af do zewnętrznego punktu dostępowego,

e) Zewnętrzne punkty dostępowe zapewniające funkcję backhaulingu bezprzewodowego,

f) Osłona IP-67 z filtrem UV

g) Temperatura robocza: -30C do +60C

h) Grzałka elektryczna do zimnego rozruchu

i) Wzmocniona obudowa - ochrona przed wyładowaniami elektrostatycznymi (ESD), komponenty klasy przemysłowej
j) Filtry do eliminacji zakłóceń LTE

7. Wymagania dodatkowe (funkcjonalne)

a) Wykonawca zapewni kontroler Wifi działający w oparciu o technologię cloud computing (chmura) pochodzący od tego samego producenta co urządzenia dostępowe lub posiadający pisemne potwierdzenie Producenta o kompatybilności.