URZĄD PATENTOWY
RZECZYPOSPOLITEJ POLSKIEJ

al. Niepodległości 188/192
00-950 Warszawa, skr. poczt. 203
tel.: (+48) 22 579 05 55 | fax: (+48) 22 579 00 01
e-mail: kontakt@uprp.gov.pl | www.uprp.gov.pl

Dyrektor Generalny

Warszawa, 19.08.2026 r.

Dot. postępowania nr BG-PZ.26.25.2026 prowadzonego w trybie przetargu nieograniczonego pn. „Dostawa, wdrożenie i konfiguracja urządzenia deszyfrującego ruch sieciowy TLS".

Zmiana treści specyfikacji warunków zamówienia (SWZ) przedłużenie terminu składania ofert

Działając na podstawie 286 ust. 1 i 3 w zw. z art. art. 284 ust. 1 ustawy z 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2026 r. poz. 793) Zamawiający udziela odpowiedzi na pytanie Wykonawcy (zawarte w załączonym pliku „pytanie.pdf") dotyczące treści SWZ poprzez zmianę jej treści i przedłuża termin składania ofert **do 24 sierpnia 2026 r. do godz. 10:00**. Otwarcie ofert nastąpi **24 sierpnia 2026 r. o godz. 10:30**. Termin związania ofertą: 17 września 2026 r.

Zmiany w Załączniku nr 1 do SWZ (Opis Przedmiotu Zamówienia):

Rozdział I zmienia brzmienie
z:

I. Urządzenie deszyfrujące ruch sieciowy TLS– minimalne wymagania

1. *Urządzenie wraz z zainstalowanym systemem operacyjnym umożliwi automatyczne rozszywanie ruchu TLS w celu przekazania go w trybie in-line do systemów analizy oraz blokowania szkodliwego oprogramowania a następnie ruch zostanie powrotnie przekazany do tego samego urządzenia rozszywającego, zostanie zaszyfrowany i przekazany do dalszej komunikacji.*
2. *Systemy analizy oraz blokowania szkodliwego oprogramowania dla których oferowane urządzenie ma przekazywać rozszyty ruch TLS w trybie in-line to w kolejności; IPS ForcePoint, Next Generation Firewall FortiGate, Fidelis Cybersecurity Sensor Direct. Pierwszy system bezpieczeństwa jest połączony z deszyfratorem TLS bezpośrednio. Transmisja pomiędzy deszyfratorem TLS a pierwszym systemem bezpieczeństwa realizowana jest obecnie za pomocą połączenia miedzianego o przepustowości 1 Gb/s. Następnie ruch z pierwszego systemu bezpieczeństwa jest przekazywany do drugiego systemu bezpieczeństwa za pośrednictwem przełącznika sieciowego. Na tym odcinku*

transmisja realizowana jest z wykorzystaniem interfejsów optycznych. Z drugiego systemu bezpieczeństwa ruch jest następnie przekazywany do trzeciego systemu bezpieczeństwa, również za pośrednictwem przełącznika sieciowego. Na tym odcinku transmisja również realizowana jest z wykorzystaniem interfejsów optycznych. Następnie ruch z trzeciego systemu bezpieczeństwa jest przekazywany bezpośrednio do deszyfratora TLS. Transmisja pomiędzy trzecim systemem bezpieczeństwa a deszyfratorem TLS realizowana jest obecnie za pomocą połączenia miedzianego o przepustowości 1 Gb/s. Opisany powyżej scenariusz i kolejność połączeń są takie same dla obu kierunków transmisji, zarówno dla ruchu kierowanego do Internetu, jak i dla ruchu przychodzącego z Internetu.

Zamawiający informuje, że obecna konfiguracja przedstawia się następująco:

a. *Rodzaj medium transmisyjnego: obecnie komunikacja pomiędzy deszyfratorem TLS a integrowanymi urządzeniami realizowana jest z wykorzystaniem okablowania miedzianego (Copper). Jednocześnie Zamawiający wymaga, aby oferowane rozwiązanie zapewniało możliwość realizacji połączeń z wykorzystaniem interfejsów optycznych.*
b. *Wymagana przepustowość interfejsów: obecnie wykorzystywane są połączenia o przepustowości 1 Gb/s. Oferowane urządzenie musi jednak zapewniać możliwość rozbudowy i zwiększenia przepustowości, w szczególności poprzez obsługę interfejsów 1/10/25 Gb/s.*
c. *Typ portów: obecnie połączenia realizowane są za pomocą portów RJ45. Zamawiający wymaga jednak, aby urządzenie posiadało możliwość zastosowania interfejsów SFP/SFP+/SFP28, umożliwiających obsługę odpowiednio przepustowości 1/10/25 Gb/s.*
d. *Standard optyczny: w przypadku zastosowania połączeń światłowodowych Zamawiający wykorzystuje światłowód wielomodowy (MM) oraz standard optyczny SR.*
e. *Standard patchcordów: w przypadku zastosowania połączeń światłowodowych należy przewidzieć patchcordy zakończone złączami LC-LC Duplex, odpowiednie do zastosowanego rodzaju włókna i standardu optycznego.*
f. *Wymagana długość patchcordów: z uwagi na fakt, że urządzenia będą zlokalizowane w jednej szafie teleinformatycznej, wymagana długość pojedynczego patchcordu nie powinna przekraczać 2 m.*
g. *Topologia i liczba połączeń: deszyfrator TLS przekazuje odszyfrowany ruch w trybie inline przez trzy systemy bezpieczeństwa, zgodnie z określoną kolejnością przepływu ruchu.*

3. *Zamawiający wymaga jednak, aby oferowane urządzenie zapewniało możliwość zwiększenia przepustowości oraz przejścia na interfejsy optyczne, bez konieczności zmiany opisanej koncepcji realizacji ruchu inline.*
4. *Wykrywanie i deszyfrowanie komunikacji TLS/SSL musi być realizowane za pomocą dedykowanego urządzenia sprzętowego.*
5. *Minimalna wydajność urządzenia:*

a) *Przepustowość L3 inline (deszyfrowanie ruchu): do 4,8 Gbps,*
b) *Przepustowość L3 inline + 1 usługa L2 (np. IPS): do 3,5 Gbps,*
c) *Przepustowość L3 inline + 2 usługi L2 (np. IPS + NGFW): do 2,8 Gbps,*
d) *Dla każdej dodatkowej usługi warstwy L2 przepustowość może ulec redukcji o max. ok. 1,3 Gbps,*
e) *Nowe transakcje TLS/SSL na sekundę (TPS) w trybie L3 inline : min. 6 000.*

6. *Urządzenie musi wspierać aktualne standardy bezpieczeństwa i szyfrowania:*
   a) *TLS 1.3, TLS 1.2,*
   b) *HTTP/2 i HTTP/3 (QUIC),*
   c) *Rozpoznawanie i dekodowanie ruchu szyfrowanego niezależnie od portu i aplikacji.*
7. *Urządzenie musi być wyposażone w mechanizm zapewniający ciągłość przepływu ruchu w przypadku awarii pojedynczego portu lub utraty łączności, np. poprzez sprzętowy bypass (Fail-to-Wire) lub inne rozwiązanie gwarantujące nieprzerwaną transmisję ruchu.*
8. *Urządzenie musi być wyposażone co najmniej w następujące porty sieciowe:*
   a) *Min. 4 x 1Gb/s RJ45,*
   b) *Min. 4 x 1/10/25 Gb/s (SFP/SFP+/SFP28).*
9. *Urządzenie musi wspierać zarządzanie certyfikatami w zakresie:*
   a) *Automatycznego generowania certyfikatów self-signed,*
   b) *Importu certyfikatów i kluczy prywatnych,*
   c) *Generowania CSR i integracji z CA Zamawiającego.*
10. *Urządzenie musi być wyposażone w mechanizm kategoryzacji domen, z możliwością wykluczania z procesu deszyfracji ruchu do stron o charakterze finansowym, medycznym, religijnym, rządowym. Kategorie muszą być stale aktualizowane przez producenta, z możliwością edycji i definiowania własnych list.*
11. *Urządzenie musi umożliwiać budowanie White/Black List w oparciu o:*
    a) *Adresy IP (źródłowe, docelowe, podsieci),*
    b) *Nazwy domen (wildcard, np. *.uprp.gov.pl),*
    c) *Kategorie domen,*
    d) *Aplikacje (rozpoznawanie L7).*

na:

I. Urządzenie deszyfrujące ruch sieciowy TLS– minimalne wymagania

1. Urządzenie wraz z zainstalowanym systemem operacyjnym umożliwi automatyczne rozszyfrowanie ruchu TLS w celu przekazania go w trybie in-line do systemów analizy oraz blokowania szkodliwego oprogramowania a następnie ruch zostanie powrotnie przekazany do tego samego urządzenia rozszyfrowującego, zostanie zaszyfrowany i przekazany do dalszej komunikacji.

Rozwiązanie musi umożliwiać realizację procesu:

ruch szyfrowany → deszyfrowanie → urządzenia bezpieczeństwa → ponowne

szyfrowanie → dalsza transmisja

dla obu kierunków transmisji.

Urządzenie musi umożliwiać definiowanie kolejności oraz liczby systemów bezpieczeństwa znajdujących się w łańcuchu przetwarzania ruchu.

2. Urządzenie musi umożliwiać przekazywanie odszyfrowanego ruchu TLS/SSL w trybie inline do co najmniej trzech kolejnych systemów bezpieczeństwa, z możliwością określenia kolejności ich występowania w łańcuchu przetwarzania.
   Rozwiązanie musi umożliwiać realizację następującego logicznego modelu przepływu:

   deszyfrator TLS → system bezpieczeństwa 1 → system bezpieczeństwa 2 → system bezpieczeństwa 3 → deszyfrator TLS

   oraz analogicznego przepływu dla przeciwnego kierunku transmisji.

   Oferowane urządzenie musi umożliwiać współpracę z istniejącymi systemami bezpieczeństwa Zamawiającego, w szczególności z:
   - IPS Forcepoint,
   - Next Generation Firewall FortiGate,
   - Fidelis Cybersecurity Sensor Direct,

   z wykorzystaniem standardowych interfejsów i mechanizmów transmisji Ethernet.

   Dopuszcza się realizację połączeń pomiędzy urządzeniem deszyfrującym a systemami bezpieczeństwa z wykorzystaniem interfejsów miedzianych lub optycznych, odpowiednio do możliwości oferowanego rozwiązania.
   Obecna infrastruktura Zamawiającego wykorzystuje połączenia 1 Gb/s realizowane za pomocą interfejsów RJ45. Oferowane rozwiązanie musi umożliwiać wykorzystanie istniejącej infrastruktury oraz zapewniać możliwość jej rozbudowy.
   a. Urządzenie musi umożliwiać realizację połączeń za pomocą interfejsów:
      - miedzianych Ethernet,
      - optycznych Ethernet.
   b. Oferowane rozwiązanie musi obsługiwać interfejsy o przepustowości co najmniej:
      - 1 Gb/s,
      - 10 Gb/s,
      - 25 Gb/s,

      odpowiednio do zastosowanego typu interfejsu.
   c. Urządzenie musi umożliwiać zastosowanie modułów/interfejsów SFP, SFP+ lub SFP28 odpowiednich do wymaganej przepustowości.
      Rozwiązanie musi umożliwiać zastosowanie optyki zgodnej z infrastrukturą Zamawiającego, w szczególności dla transmisji wielomodowej MM w

standardzie SR.

d. Dla połączeń optycznych Zamawiający przewiduje wykorzystanie patchcordów zakończonych złączami LC-LC Duplex, odpowiednich do zastosowanego typu włókna i standardu optycznego.
e. Z uwagi na lokalizację urządzeń w jednej szafie teleinformatycznej wymagane jest zapewnienie możliwości wykonania połączeń z wykorzystaniem patchcordów o długości nie większej niż 2 m.
f. Urządzenie musi umożliwiać realizację łańcucha inline składającego się z co najmniej trzech systemów bezpieczeństwa, z możliwością określenia kolejności przepływu ruchu.

3. Oferowane urządzenie musi zapewniać możliwość zwiększenia przepustowości oraz przejścia z interfejsów miedzianych na optyczne bez konieczności zmiany funkcjonalnego modelu realizacji inspekcji inline.
   Rozbudowa musi zachować możliwość:
   - deszyfrowania ruchu TLS/SSL,
   - przekazywania odszyfrowanego ruchu do systemów bezpieczeństwa,
   - odbierania ruchu z systemów bezpieczeństwa,
   - ponownego szyfrowania ruchu,
   - przekazywania ruchu do dalszej komunikacji.

   Dopuszcza się realizację rozbudowy poprzez wymianę lub dodanie interfejsów, modułów, kart lub innych elementów sprzętowych przewidzianych przez producenta dla oferowanej platformy.

4. Wykrywanie oraz deszyfrowanie komunikacji TLS/SSL musi być realizowane przez dedykowane urządzenie sprzętowe lub dedykowany moduł sprzętowy przeznaczony przez producenta do realizacji funkcji inline TLS/SSL decryption.

   Nie dopuszcza się rozwiązania, w którym funkcja deszyfrowania jest realizowana wyłącznie przez oprogramowanie uruchomione na ogólnym serwerze bez dedykowanej funkcji sprzętowej producenta.
5. Urządzenie musi zapewniać następującą minimalną wydajność dla ruchu TLS/SSL w trybie inline:
   a. Przepustowość deszyfrowania ruchu TLS/SSL w konfiguracji bez dodatkowych urządzeń bezpieczeństwa w łańcuchu inspekcji: **minimum 4,8 Gbps**,
   b. Przepustowość deszyfrowania ruchu TLS/SSL przy zastosowaniu co najmniej jednego zewnętrznego systemu bezpieczeństwa pracującego inline: **minimum 3,5 Gbps**,
   c. Przepustowość deszyfrowania ruchu TLS/SSL przy zastosowaniu co najmniej dwóch zewnętrznych systemów bezpieczeństwa pracujących inline: **minimum 2,8 Gbps,**
   d. Urządzenie musi umożliwiać utworzenie łańcucha obejmującego co najmniej trzy systemy bezpieczeństwa pracujące inline.
      Oferent musi podać deklarowaną przez producenta przepustowość dla konfiguracji obejmującej trzy systemy bezpieczeństwa pracujące inline.
      Dodanie kolejnych systemów bezpieczeństwa do łańcucha nie może

powodować ograniczenia możliwości realizacji funkcji inline TLS/SSL decryption poniżej wartości wymaganej dla danego scenariusza.

e. Urządzenie musi obsługiwać minimum: **6 000 nowych sesji TLS/SSL na sekundę (TPS)** w konfiguracji inline.
f. W przypadku podawania parametrów wydajnościowych przez producenta w odniesieniu do określonej metodologii testowej, oferent zobowiązany jest wskazać:
   - model urządzenia,
   - zastosowaną konfigurację sprzętową,
   - wersję oprogramowania,
   - zastosowaną metodę szyfrowania,
   - sposób pomiaru TPS,
   - warunki testu,
   - czy podana wartość dotyczy ruchu jednokierunkowego czy dwukierunkowego.

Parametry wydajnościowe muszą dotyczyć oferowanego modelu i oferowanej konfiguracji urządzenia.

6. Urządzenie musi wspierać:
   a. TLS 1.3 oraz TLS 1.2.
   b. Protokoły aplikacyjne HTTP/1.1 oraz HTTP/2.
   c. Rozpoznawanie ruchu TLS/SSL niezależnie od zastosowanego numeru portu TCP.
   d. Rozpoznawanie ruchu aplikacyjnego na podstawie analizy protokołu, a nie wyłącznie na podstawie numeru portu.
   e. Rozpoznawanie ruchu QUIC/HTTP/3 oraz możliwość zastosowania wobec niego skonfigurowanej polityki bezpieczeństwa, w szczególności:
      - przepuszczenia ruchu,
      - zablokowania ruchu,
      - wyłączenia ruchu z procesu deszyfracji,
      - skierowania ruchu do zdefiniowanego procesu dalszego przetwarzania,
      - zgodnie z funkcjonalnościami oferowanego rozwiązania.

      Nie wymaga się deszyfrowania QUIC/HTTP/3, o ile producent nie zapewnia takiej funkcjonalności.
7. Urządzenie musi zapewniać mechanizm zapewniający ciągłość przepływu ruchu w przypadku:
   - awarii urządzenia,
   - awarii pojedynczego interfejsu,
   - utraty zasilania,
   - utraty komunikacji z urządzeniem bezpieczeństwa,

   poprzez sprzętowy mechanizm bypass, Fail-to-Wire, Fail-to-Network, Fail-to-Appliance lub rozwiązanie funkcjonalnie równoważne.
   Mechanizm musi zapewniać automatyczne przekazanie ruchu z pominięciem niedostępnego elementu infrastruktury, zgodnie z konfiguracją urządzenia.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

8. Urządzenie musi zapewniać możliwość realizacji wymaganej topologii inline z wykorzystaniem interfejsów miedzianych oraz optycznych.
   Oferowane rozwiązanie musi obsługiwać:
   a. co najmniej 4 interfejsy Ethernet 1 Gb/s umożliwiające realizację połączeń miedzianych RJ45;
   b. co najmniej 4 interfejsy optyczne obsługujące przepustowości 1/10/25 Gb/s, z wykorzystaniem odpowiednich modułów SFP/SFP+/SFP28;
   c. jednoczesną pracę interfejsów miedzianych i optycznych;
   d. standardy optyczne kompatybilne z infrastrukturą Zamawiającego, w szczególności 10/25 Gb/s SR dla światłowodu wielomodowego.
   Dopuszcza się realizację wymaganej liczby interfejsów poprzez zastosowanie modułów, kart lub innych elementów rozszerzających przewidzianych przez producenta dla oferowanego modelu, pod warunkiem zachowania wymaganej funkcjonalności oraz wydajności.

9. Urządzenie musi zapewniać zarządzanie certyfikatami wykorzystywanymi do realizacji funkcji TLS/SSL decryption, w szczególności:
   - automatyczne generowanie certyfikatów self-signed;
   - import certyfikatów oraz kluczy prywatnych;
   - generowanie CSR;
   - możliwość wykorzystania certyfikatów wystawionych przez CA Zamawiającego;
   - możliwość zarządzania certyfikatami wykorzystywanymi do deszyfrowania ruchu TLS/SSL.

10. Urządzenie musi posiadać mechanizm kategoryzacji domen/hostów umożliwiający wykorzystanie kategorii w politykach bezpieczeństwa oraz politykach deszyfracji.
    Mechanizm musi umożliwiać wyłączenie z procesu deszyfracji ruchu kierowanego do określonych kategorii domen, w szczególności kategorii:
    - finansowych,
    - medycznych,
    - religijnych,
    - rządowych,

    lub równoważnych kategorii zdefiniowanych w bazie producenta.
    Baza kategorii musi być aktualizowana przez producenta.
    System musi umożliwiać:
    - tworzenie własnych kategorii,
    - definiowanie własnych list domen,
    - dodawanie wyjątków,
    - wykorzystanie kategorii w politykach deszyfracji.

11. Urządzenie musi umożliwiać budowanie polityk dopuszczania, blokowania, pomijania procesu deszyfracji lub kierowania ruchu do określonego łańcucha bezpieczeństwa na podstawie co najmniej:
    a. adresu IP źródłowego i docelowego, w tym podsieci;

b. nazwy domeny, w tym nazw zawierających wildcard, np.:
   - *.uprp.gov.pl;
c. kategorii domen/hostów;
d. identyfikacji aplikacji lub protokołu warstwy aplikacyjnej L7;
e. numeru portu oraz protokołu transportowego;
f. kombinacji co najmniej dwóch spośród powyższych kryteriów.
g. Polityki muszą umożliwiać co najmniej:
   - Allow / White List,
   - Block / Black List,
   - Bypass / wyłączenie z deszyfracji,
   - skierowanie ruchu do określonego łańcucha urządzeń bezpieczeństwa.

DYREKTOR GENERALNY

Marcin Dobruk