Załącznik nr 2 do SIWZ

Minimalne wymagania dla systemu bezpieczeństwa

I. Ogólne dotyczące informacji zawartych w specyfikacji

Wszystkie opisane funkcjonalności i parametry są wymaganiami minimalnymi. Wykonawca może dostarczyć rozwiązanie o parametrach równoważnych lub lepszych, które nie spowodują utraty funkcjonalności i wydajności.

II. Koncepcja ogólna rozwiązania

Celem projektu jest wyposażenie Regionalnej Izby Obrachunkowej w Lublinie w ***system bezpieczeństwa*** mający na celu zintegrowanie wszystkich ***lokalizacji RIO*** oraz objęcie ich ***aktywną ochroną***.

System bezpieczeństwa musi zrealizować ***integrację lokalizacji*** za pomocą połączenia ich tunelami VPN

- zestawianymi przez ***urządzenia*** metodą site to site przy pomocy IPSec VPN
  - ***ZRIO*** z ***GRIO***
  - ***IRIO*** z ***GRIO***
- z ***LNZB*** do ***GRIO*** lub ***ZRIO*** przy pomocy SSL VPN inicjowanymi przez oprogramowanie klienckie zainstalowane na komputerze znajdującym się w ***LNZB***.

W celu zapewnienia maksymalnej elastyczności podłączania do sieci ***urządzenia*** powinny obsługiwać po stronie WAN: port Ethernet, wbudowany lub przyłączany przez port USB modem 3G. W odniesieniu do ***IRIO*** system musi umożliwiać podłączenie do sieci internet (WAN) poprzez sieci WiFi dostępne w ***j.s.t.*** - dopuszcza się doposażenie urządzenia w dodatkowy sprzęt (karta USB WiFi lub inne) mogący być klientem sieci WiFi w celu zestawienia połączenia WAN przez sieć WiFi.

Integracja lokalizacji musi być realizowana również w przypadku łącz asymetrycznych ze zmiennym adresem IP, w szczególności dostarczane przez TP SA typu VDSL, aDSL, DSL, oraz jako łącza zapasowe modemy 3G/4G.

Urządzenia w ***GRIO, ZRIO*** oraz ***IRIO***, tj. w każdej ***LRIO,*** muszą

1. posiadać posiadać funkcję podłączania ich do internetu za pomocą modemu 3G instalowanego w ***urządzeniu*** poprzez port USB;
2. obsługiwać mechanizm dynamic DNS;
3. posiadać funkcjonalność jednoczesnego uruchomienia połączenia poprzez kilka łącz WAN przy czym
   a) w przypadku jednoczesnego działania w urządzeniu kilku łącz WAN ruch sieciowy musi być rozkładany pomiędzy łącza wg ustalonego priorytetu.
   b) mechanizm definiowania priorytetów musi uwzględniać rodzaj ruchu sieciowego oraz jego źródło i cel.
   c) w przypadku awarii łącza o wyższym priorytecie ruch musi być automatycznie przekierowany na inne łącze WAN.

System bezpieczeństwa musi

1. obejmować ***aktywną ochroną*** sieci w ***GRIO***, ***ZRIO*** oraz ***IRIO*** przy czym ***aktywna ochrona*** w każdej ***lokalizacji RIO*** musi być realizowana w pełnym zakresie, nawet w przypadku braku połączenia z ***GRIO***.
2. zapewnić ***aktywną ochronę*** dla użytkowników znajdujących się w lokalizacjach zdalnych przyłączonych do ***GRIO*** kanałami VPN, w tym również użytkowników znajdujących się w ***LNZB.***.
3. posiadać konsolę centralnego zarządzania
4. być wyposażony w ***rejestrator zdarzeń*** służący do logowania informacji związanych z
   a. kondycją ***urządzenia*** oraz każdego z jego modułów zdarzeń
      i. sprzętowych,
      ii. bezpieczeństwa, w tym logowanie się ***operatorów*** do ***urządzeń***,
      iii. związanych z działaniami wykonywanych przez ***operatorów*** po zalogowaniu się do ***urządzenia***, w tym modyfikacji ustawień,
   b. realizacją zadań wykonywanych przez moduł ***systemu bezpieczeństwa***
      i. zalogowane zdarzenia i pakiety muszą zawierać informacje pozwalające na powiązanie ich z ***regułą bezpieczeństwa***, sygnaturą IPS/IDS, antywirusów, nazwą użytkownika, nazwa aplikacji.

Urządzenia dla ***IRIO*** oraz ***ZRIO*** muszą posiadać porty ethernet do bezpośredniego podłączania komputerów użytkowników do tego ***urządzenia*** oraz pozwalać na:

1) podłączenie do niego komputerów wszystkich użytkowników danej z ***ZRIO*** lub ***IRIO*** za pomocą WiFi;
2) nawiązanie bezpiecznego połączenia VPN z ***GRIO***;
3) utworzenie polityki zezwalającej na bezpośredni dostęp do Internetu z komputerów w ***IRIO*** z pominięciem tunelu VPN łączącego ***IRIO*** z ***GRIO***;
4) objęcie aktywną ochroną, nawet w przypadku braku połączenia z **GRIO**.

Dodatkowo***, urządzenia*** dla każdego z ***IRIO*** muszą pozwalać na:

1) odizolowanie komputerów użytkowników od sieci LAN w ***j.s.t.***;
2) podłączenie ***urządzenia*** do LAN w **j.s.t.** zarówno za pomocą WiFi jak i portu ethernet.

Urządzenia muszą wspierać następujące tryby pracy: routing z NAT (warstwa 3), bridge (warstwa 2) oraz tryb mieszany (routing i bridge jednocześnie).

System bezpieczeństwa musi być licencjonowany dla nielimitowanej liczby hostów i użytkowników.

Urządzenia do poszczególnych lokalizacji muszą być dobrane z uwzględnieniem ilości użytkowników oraz rodzaju obciążenia i charakteru pracy w danej lokalizacji.

System bezpieczeństwa musi zapewnić powyższe funkcjonalności dla wszystkich lokalizacji według szczegółów opisanych dalej.

III. Szczegółowe parametry dla *systemu bezpieczeństwa* i *urządzeń* składowych

VPN

Urządzenia muszą

1. zestawiać następujące typy połączeń VPN: IPsec (Site-to-site, Client-to-site), L2TP i PPTP;
2. obsługiwać następujące algorytmy: DES, 3DES, AES;
3. posiadać wbudowane, własne centrum autoryzacji;
4. posiadać funkcję wykorzystywania zewnętrznych centrów certyfikacji w procesie autentykacji;

5. realizować uwierzytelnianie użytkowników VPN za pomocą certyfikatów cyfrowych i/lub kont logowania zarówno wbudowanych jak i kont ***AD***;
6. obsługiwać ogólnodostępnych klientów IPSec VPN, tj. do nawiązywania połączeń VPN nie będzie wymagane używanie dedykowanego oprogramowania producenta urządzenia;
7. posiadać wbudowany moduł SSL-VPN;
8. posiadać funkcję skanowania antywirusowego tuneli VPN (IPsec/L2TP/PPTP);
9. monitorować stan realizowanych połączeń VPN oraz automatycznie nawiązywać zapasowe połączenia VPN w przypadku przerwania połączenia;
10. posiadać funkcję zarządzania pasmem dla każdego tunelu VPN;
11. obsługiwać funkcję NAT Traversal w przypadku działania w roli bramy VPN;
12. zapewniać budowanie tuneli VPN w oparciu o protokoły: TCP, UDP, ESP, TCP/UDP;

Aktywna ochrona

Urządzenia muszą obsługiwać przynajmniej następujące ***strefy bezpieczeństwa*** LAN, WAN, DMZ, VPN, WLAN, VLAN.

Urządzenia muszą pozwalać na tworzenie ***reguł bezpieczeństwa*** dla wszystkich modułów ***aktywnej ochrony*** oraz na zdefiniowanie kryterium ***reguły bezpieczeństwa*** w oparciu o: każdą ze ***stref bezpieczeństwa***, źródłowe i docelowe adresy IP, protokoły sieciowe, identyfikatory użytkowników, identyfikatory grup użytkowników.

Aktywna ochrona w poszczególnych ***LRIO*** musi być

1. zrealizowana w formie sprzętowej z zabezpieczonym specjalizowanym systemem operacyjnym, tzn. nie może wymagać od użytkownika instalacji osobnego systemu operacyjnego oraz nie może być zainstalowane na systemie operacyjnym ogólnego przeznaczenia;
2. realizowana w każdej ***LRIO*** przez pojedyncze ***urządzenia***.

SIF

Urządzenia muszą posiadać

1. firewall obsługujący wszystkie połączenia wychodzące i przychodzące ze wszystkich ***stref bezpieczeństwa***;
2. wbudowany analizator pakietów (sniffer) uruchamiany z graficznej konsoli operatora i z wiersza poleceń urządzenia.

Urządzenia muszą obsługiwać

1. następujące protokoły routingu: RIP1, RIP2, OSPF, BGP4;
2. konfigurację routingu statycznego i dynamicznego;
3. translacje adresów NAT, PAT;
4. nie mniej niż 254 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.

Urządzenia muszą realizować kontrolę przepustowości łącz (QoS) w oparciu o: identyfikator użytkowników, identyfikator grupy użytkowników, nazwę aplikacji, identyfikator reguły zapory sieciowej.

Konfigurator reguł firewalla musi posiadać funkcję pozwalającą na przypisanie niezależnej ochrony dla każdej reguły, tj. indywidualnie dla każdej reguły włączyć/wyłączyć i konfigurować:

1) skanowanie ***MAV*** i ***MAS*** niezależnie dla każdego z protokołów SMTP, POP3, IMAP, FTP, HTTP, HTTPS;
2) zarządzanie pasmem QoS,
3) odrębne reguły filtrów aplikacji,
4) filtrów ***MKSI***
5) reguły ***IPS***.

IPS

Urządzenia muszą

1. zapewniać ochronę przed atakami typu DoS/DDoS: IP spoofing. SYN flooding, flood ping i innymi, oraz przed skanowaniem portów i adresów;
2. odrębnie dla każdej reguły zezwalać na zmianę domyślnej reakcji ***systemu bezpieczeństwa*** w przypadku wykrycia ruchu opisanego regułą;
3. obsługiwać dodawanie sygnatur ataków przez administratora;
4. wysyłać alerty e-mailem lub poprzez SNMP w przypadku wykrycia prób ataków.

Producent urządzenia w ramach licencji musi dostarczać sygnatury ataków przez cały czas trwania licencji.

MAV

Urządzenia muszą

1. skanować protokoły: SMTP, POP3, IMAP, FTP, HTTP, HTTPS;
2. posiadać funkcję dodawania podpisu/stopki o konfigurowalnej treści do wysyłanych wiadomości email z informacją o sprawdzeniu jej filtrem antywirusowym;

Dla protokołów POP3 i IMAP ***MAV*** powinien usuwać zawirusowany załącznik i przesłać odpowiednią informację do odbiorcy i administratora.

MAS

Urządzenia muszą

1. skanować następujące protokoły: POP3, IMAP, SMTP;
2. dla autoryzowanego ruchu w SMTP ***MAS*** musi posiadać funkcję włączenia/wyłączenia skanowania;
3. współpracować z bazą RBL;
4. pozwalać na tworzenie białych i czarnych list adresów IP i e-mail;
5. zapewniać wykrywanie spamu przynajmniej w języku polskim i angielskim.

MKSI

Urządzenia muszą

1. sprawdzać strony internetowe pod kątem rozpoznawania witryn potencjalnie niebezpiecznych, tj. stron szpiegujących, zawierających złośliwe oprogramowanie lub treści niedozwolone;
2. pozwalać na
   a. dodawanie przez administratora własnych kategorii oraz tworzenie wyjątków dla zdefiniowanych przez producenta i siebie kategorii stron;
   b. przypisywanie stron znajdujących się w bazie kategorii do białych lub czarnych list;
   c. zdefiniowanie kryterium reguły bezpieczeństwa modułu ***MKSI*** w oparciu o przynależność strony zarówno do kategorii jak i rodzaju listy.

Kontrola aplikacji

Urządzenia muszą

1. identyfikować aplikacje na podstawie głębokiej analizy pakietów niezależnie od wykorzystywanego portu, protokołu i szyfrowania;
2. posiadać funkcję
   a) blokowania ruchu generowanego przez:
      i) aplikacje, które pozwalają na transfer plików, przynajmniej P2P;
      ii) komunikatory internetowe, przynajmniej Skype, Gadu-gadu;
      iii) proxy uruchamiane poprzez przeglądarki internetowe;
      iv) streaming media (radio i telewizja internetowa, inne portale z streamujące treści multimedialne, w tym przynajmniej Youtube;
   b) kontroli dostępu do aplikacji osadzonych na stronach i portalach internetowych, przynajmniej WebGaduGadu;

c) szczegółowej kontroli dostępu do portali społecznościowych, w tym przynajmniej do Facebooka. Kontrola musi być realizowana przynajmniej na poziomie zamieszczania postów, czatu, uruchamiania aplikacji, uruchamiania gier, transfer plików graficznych i wideo;

3. pozwalać na zdefiniowanie kryterium reguły bezpieczeństwa modułu ***MKAI*** w oparciu o aplikację jak i grupę aplikacji.

IV. Współpraca ze środowiskiem terminalowym

System bezpieczeństwa musi posiadać funkcjonalność pozwalającą na powiązanie aktywności sieciowej serwerów terminalowych (MS Terminal Server, Citrix) z identyfikatorami zalogowanych na nich użytkowników, obejmujących zdarzenia wykryte na urządzeniach przez wszystkie moduły ***aktywnej ochrony***.

V. Uwierzytelnianie użytkowników

Urządzenia muszą pozwalać na

1. uwierzytelnianie użytkowników poprzez Windows NTLM, Active Directory, LDAP, Radius oraz lokalną bazę użytkowników w urządzeniu;
2. automatyczne uwierzytelnianie użytkowników w oparciu o Single Sign On.
3. utworzenie reguł zezwalających na zalogowanie na podstawie identyfikatora użytkownika oraz adresów IP.

Urządzenia muszą obsługiwać uwierzytelnianie w środowisku cienkiego klienta (Microsoft TSE, Citrix).

VI. Zarządzanie

System bezpieczeństwa musi pozwalać na

1. tworzenie kont administracyjnych o różnych uprawnieniach.
2. definiowanie polityk hasłowych oraz automatyczne wylogowanie administratorów po określonym czasie bezczynności.

System bezpieczeństwa musi

1. obsługiwać protokół SNMP v1, v2 i v3
2. posiadać funkcję monitorowania w czasie rzeczywistym stanu urządzeń, w tym przynajmniej użycia CPU, RAM, obciążenie interfejsów sieciowych.

Urządzenia muszą posiadać funkcję

1. przechowywania przynajmniej dwóch wersji firmware i uruchomienie w razie potrzeby dowolnej z tych wersji;
2. automatycznego wykonywania kopii zapasowej konfiguracji ***urządzeń***.

Logowanie administratorów do ***urządzeń*** musi odbywać się przynajmniej poprzez jeden z następujących kanałów komunikacyjnych: HTTPS, dedykowaną aplikację.

VII. Centralne zarządzanie, logowanie i korelacja

System(y) zarządzający, monitorujący, gromadzący logi i generujący raporty musi(szą)

1. mieć dostęp danych pochodzących ze wszystkich elementów ***systemu bezpieczeństwa***;
2. pochodzić od tego samego producenta, co elementy aktywne i muszą być dedykowane dla ***systemu bezpieczeństwa***;
3. być zoptymalizowane do uruchomienia przynajmniej na VMware ESXi 5.x w przypadku dostarczenia ich w postaci maszyny wirtualnej.

System centralnego zarządzania musi posiadać

1. funkcjonalność pozwalającą na
   a) modyfikowanie każdego aspektu działania ***systemu bezpieczeństwa*** z jednej centralnej konsoli;

   b) tworzenie szablonów ustawień i równoczesnej zmiany tych samych ustawień na dowolnej ilości ***urządzeń*** wchodzących w skład ***systemu bezpieczeństwa***;
   c) zarządzania wieloma firewallami (serwerami usług) z jednej konsoli administracyjnej (konfigurowanie i monitorowanie parametrów systemu, firewalla, serwera VPN).
2. mechanizm administracji oparty na rolach
3. funkcję
   a) powiadamiania o zdarzeniach przez email, SNMP;
   b) aktualizacji i zmiany systemu poprzez WebUI;
   c) przywracania systemu.

Moduł gromadzący logi musi realizować funkcje
1. zbierania (gromadzenie, przechowywanie) logów;
2. podgląd logowanych zdarzeń w czasie rzeczywistym;
3. przechowywania logów na dodatkowych zewnętrznych urządzeniach.

W ramach centralnego systemu zarządzania, logowania, raportowania ***system bezpieczeństwa*** musi posiadać centralny dziennik zdarzeń oraz wspierać
1. logowanie na serwerze syslog zdarzeń związanych z: MAV, MAS, MKSI, IPS, SIF;
2. zbieranie logów z urządzeń UTM.

System logowania musi posiadać funkcję cyklicznego eksportu zgromadzonych logów do zewnętrznych systemów przechowywania danych w celu ich składowania przez dłuższy okres czasu.

Moduł raportujący musi
1. generować raporty
   a) zarówno na podstawie danych bieżących, jak i danych archiwalnych z zadanego przedziału czasu;
   b) na żądanie oraz w trybie cyklicznym;
2. zapewniać podgląd
   a) wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym zbiorczo dla wszystkich łącz ***urządzenia*** oraz indywidualnie dla każdego łącza oddzielnie;
   b) w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o adres IP , login użytkownika lub nazwę aplikacji;
3. posiadać raporty, za pomocą których administrator będzie mógł zidentyfikować użytkowników wywołujących zdarzenia zarejestrowane przez ***system bezpieczeństwa***;
4. zapisywać wygenerowane raporty do plików przynajmniej w formatach: PDF, XLS.

VIII. Wymagania specyficzne dla poszczególnych *lokalizacji RIO*

GRIO

System musi się dać w przyszłości rozbudować o kolejne elementy celem zbudowania klastra zapewniającego wysoką dostępność w trybach active-active (praca jednoczesna zwiększająca wydajność jeżeli nie ma awarii i przejęcie funkcji uszkodzonego urządzenia podczas awarii) i active-passive (przejęcie funkcji uszkodzonego urządzenia przez urządzenie pasywne).

Urządzenia muszą posiadać
1. przynajmniej 8 portów 10/100/1000 Mbps;
2. funkcję skonfigurowania każdego z portów do pracy jako WAN, LAN, DMZ, HA.

Ilość lokalizacji: 1

Parametry pracy ***urządzeń:***
1. Ilość jednocześnie uruchomionych łącz WAN: 3
2. Wydajność urządzenia:150 użytkowników.
3. Nie mniej niż 1000 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard IEEE802.1q

4. Obsługa nie mniej niż
   a) 40 000 nowych połączeń na sek
   b) 1 000 000 jednoczesnych połączeń
5. Przepustowość
   a) ***SIF***: nie mniej niż 3000 Mbps
   b) ***IPS***: nie mniej niż 950 Mbps
   c) ***MAV***: nie mniej niż 1000 Mbps
   d) tunelu IPSec VPN: nie mniej niż 450 Mbps
6. Liczba tuneli IPSec VPN: nie mniejsza niż 200.

ZRIO

Ilość lokalizacji: 4

Urządzenia muszą posiadać
1. przynajmniej 4 porty 10/100/1000 Mbps;
2. funkcję skonfigurowania każdego z portów do pracy jako WAN, LAN, DMZ;
3. wbudowany Access Point WiFi z obsługą standardów 802.11g i 802.11n.

Parametry pracy ***urządzeń:***
1. Ilość jednocześnie uruchomionych łącz WAN: 3
2. Wydajność urządzenia:20 użytkowników.

IRIO

Ilość lokalizacji: 16

Urządzenia muszą posiadać
1. przynajmniej 1 port WAN 10/100 Mbps
2. przynajmniej 1 port DMZ 10/100/1000 Mbps
3. przynajmniej 1 port LAN 10/100/1000 Mbps
4. wbudowany Access Point WiFi z obsługą standardów 802.11g i 802.11n

System bezpieczeństwa w ***IRIO*** musi równocześnie udostępniać tryb Wireless WAN (Client Mode Wireless, multi bridge(WISP/AP client). Dopuszcza się realizację tego wymagania za pomocą dodatkowego urządzenia.

Ilość jednocześnie uruchomionych łącz WAN: 2

IX. SERWIS

1. ***System bezpieczeństwa*** oraz wszystkie jego części składowe, zarówno sprzęt jak i oprogramowanie muszą
   a) być dostarczone wraz z wszelkimi licencjami niezbędnymi do uruchomienia go w pełnej funkcjonalności opisanej w SIWZ. W przypadku licencji ograniczonych czasowo, okres ich ważności nie może być krótszy niż 5 lat;
   b) być objęte pięcioletnią gwarancją i wsparciem technicznym Oferenta
      i) realizowanych na terenie Rzeczpospolitej Polskiej w języku polskim,
      ii) świadczonych w dni robocze od poniedziałku do piątku w godzinach 8:00-17:00,
      iii) polegających na
         1) naprawie lub wymianie ***urządzeń*** w przypadku ich wadliwości w przeciągu 14 dni;
         2) zapewnieniu wsparcia technicznego obejmującym diagnostykę i wymianę urządzeń w razie ich awarii;
         3) zapewnieniu konsultacji przy nieprawidłowym działaniu systemu bezpieczeństwa jako całości oraz jego elementów składowych, zarówno oprogramowania jak i ***urządzeń***
   c) posiadać możliwość odpłatnego przedłużenia okresu gwarancji i wsparcia technicznego o minimum trzy kolejne lata po wygaśnięciu gwarancji i wsparcia technicznego.

2. W czasie trwania gwarancji i wsparcia technicznego Zamawiający ma
   a) dostęp oraz prawo do korzystania z aktualizacji
      i) sygnatur antywirusowych i antyspamowych;
      ii) reguł IPS/IDS;
      iii) bazy kategorii stron;
      iv) oprogramowania
         1) systemowego ***urządzeń*** (ang. firmware upgrade);
         2) każdego oprogramowania dostarczonego wraz ***systemem bezpieczeństwa***
   b) dostęp do wsparcia technicznego Producenta świadczonego w systemie 24 godziny/dobę 7 dni w tygodniu;
3. ***System bezpieczeństwa*** musi posiadać dedykowane dla niego szkolenia prowadzone na terenie Rzeczpospolitej Polskiej w języku polskim przez trenera posiadającego certyfikat Producenta ***systemu bezpieczeństwa*** na prowadzenie szkoleń.
4. Zobowiązania Oferenta w zakresie
   a) gwarancji i wsparcia technicznego,
   b) określonym §8 umowy,

   mogą zostać przeniesione w części lub w całości z Oferenta na Dystrybutora certyfikowanego przez Producenta ***systemu bezpieczeństwa***. Warunkiem dokonania takiego przeniesienia jest dostarczenie, wraz z ofertą, oświadczenia Dystrybutora zawierającego informację o zakresie przejęcia obowiązków oraz zgodę na wzięcie na siebie wynikających z tego tytułu zobowiązań.
5. Oferent zobowiązany jest do złożenia wraz z ofertą oświadczenia Producenta ***systemu bezpieczeństwa*** potwierdzającego, że w przypadku nie wywiązania się przez Oferenta i/lub Dystrybutora z obowiązków związanych ze świadczeniem usług gwarancyjnych i wsparcia technicznego, zostaną one przejęte bezpośrednio przez Producenta bądź przez firmę wskazaną przez Producenta. W przypadku gdy Producent na terenie Rzeczpospolitej Polskiej nie posiada własnego centrum serwisowego, Oferent winien przedłożyć dokument Producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego i wsparcia technicznego na terenie Rzeczpospolitej Polskiej.

X. Szczegóły organizacyjne dostawy/oferty i inne wymagania jakościowe

Wszystkie urządzenia dostarczone w ramach ***systemu bezpieczeństwa*** muszą

- być fabrycznie nowe,
- być oznakowane symbolem CE,
- pochodzić z legalnego źródła,
- być dostarczone przez autoryzowany kanał sprzedaży producenta na terenie kraju. Zamawiający zastrzega sobie prawo do żądania potwierdzenia źródła pochodzenia urządzenia w postaci oświadczenia producenta.

1) Rozwiązanie ma posiadać certyfikację ISO 15408/Common Criteria na poziomie EAL 4+. Do oferty należy dołączyć oświadczenie o posiadaniu certyfikatu.