1. Przedmiotem zamówienia jest:
   1. dostarczenie oprogramowania PKI (ang. Public Key Infrastrukture) zgodnie ze Specyfikacją Systemu,
   2. przeprowadzenie Wdrożenia zgodnie z warunkami ppu, w tym wykonanie i dostarczenie Projektu Technicznego, Planu Testów Akceptacyjnych oraz Dokumentacji powykonawczej w formie elektronicznej;
   3. zapewnienie Zamawiającemu prawa do nieograniczonego czasowo i terytorialnie korzystania z Systemu wraz z jego dokumentacją (techniczna, użytkownika, administratora) zgodnie z ich charakterem i przeznaczeniem, (licencja obowiązująca od dnia podpisania przez Zamawiającego Protokołu Wdrożenia) na zasadach określonych w ppu oraz ogólnych warunkach producenta, w tym przekazanie dokumentu licencyjnego wystawionego przez producenta Systemu potwierdzający prawo do korzystania przez Zamawiającego z Systemu i wskazujący termin korzystania z Systemu wraz z jego dokumentacją, zgodnie z zapisami ppu i ogólnymi warunkami licencyjnymi producenta Systemu oraz sporządzoną w języku polskim (lub w języku angielskim, o ile nie istnieje polska wersja językowa) treść warunków licencyjnych producenta i ogólnych warunków korzystania z Systemu;
   4. przeniesienie na Zamawiającego autorskich praw majątkowych do Dokumentacji opracowanej przez Wykonawcę w ramach Umowy;
   5. świadczenie Gwarancji dla Systemu przez okres 36 miesięcy od dnia podpisania bez zastrzeżeń przez Zamawiającego Protokołu Wdrożenia, w tym zapewnienie świadczenia Gwarancji przez producenta Sytemu (opieki serwisowej), poprzez wydanie odpowiedniego dokumentu na rzecz Zamawiającego, potwierdzającego prawo dostępu do Gwarancji Systemu udzielanej przez producenta w ww. okresie, zgodnie z ogólnymi warunkami producenta,
   6. świadczenie na rzecz Zamawiającego Usługi wsparcia ( 200 godzin konsultacji technicznych) zgodnie z warunkami ppu, w tym przeniesienie na Zamawiającego autorskich praw majątkowych do rezultatów czynności wykonanych przez Wykonawcę w ramach Usługi Wsparcia.

**Specyfikacja Systemu**

|  |  |
| --- | --- |
| Infrastruktura Klucza Publicznego | (ang. Public Key Infrastrukture) (PKI) – w ogólności jest to zespół urządzeń, oprogramowania oraz procedur umożliwiających tworzenie, przechowywanie, zarządzanie i rozprowadzanie cyfrowych certyfikatów. |
| CA | Urząd certyfikacji ( ang. Certification Authority), który jest odpowiedzialny za wystawianie i unieważnianie certyfikatów klucza publicznego, który sam sobie poświadczył zaświadczenie certyfikacyjne i może wydawać zaświadczenia certyfikacyjne innym podmiotom świadczącym usługi certyfikacyjne. |
| TLS/SSL | (ang. Transport LAyer Security), protokół komunikacyjny zapewniający bezpieczną komunikację poprzez sieć. |
| RootCA | Główny Urząd Certyfikacji. |
| SubCA | Podrzędny Urząd Certyfikacji. |
| RA | (ang.Registration Authority),urząd rejestracji – zbiera wnioski o wydanie certyfikatu, weryfikuje tożsamość właściciela certyfikatu. |
| VA | (ang. National Validation Authority),centralny punkt walidacji danych (w tym przede wszystkim weryfikacji podpisów elektronicznych) świadczącym usługi na potrzeby elektronicznego certyfikatu. |
| SCEP | Protokół umożliwiający m.in. odbieranie wniosków o certyfikat od uwierzytelnionych klientów usługi i kierowaniu ich do urzędu CA oraz udostępniania wydanych przez urząd CA certyfikatów uwierzytelnionym klientom. |
| x.509 | X.509 to standard definiujący schemat dla certyfikatów kluczy publicznych, unieważnień certyfikatów oraz certyfikatów atrybutu służących do budowania hierarchicznej struktury PKI. |
| CRL | (ang. Certificate Revocation List), lista certyfikatów unieważnionych przez organ certyfikujących . |
| OSCP | (ang. Online Certyficate Status Protocol), protokół komunikacyjny umożliwiający walidację ważności certyfikatu |
| PKCS#10 | (ang. Certification Request Standard) standard opisujący format komunikatu żądania wystawienia certyfikatu klucza publicznego. |
| PKCS#12 | (ang*.* [Personal Information Exchange Syntax Standard](https://web.archive.org/web/20170417091802/http:/www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs12-personal-information-exchange-syntax-standard.htm)*),* standard (PFX) opisuje przechowywanie w pliku certyfikatu, klucza w jednym zaszyfrowanym pliku. |

**Rozdział I.**

**Wstęp**

Celem zamówienia jest zakup i wdrożenie w środowisku WAN rozwiązania uwierzytelnienia opartego o system certyfikacji PKI na potrzeby systemu kryptograficznego działajacego w technologii GET-VPN oraz zdalnego dostępu do infrastruktury   
z wykorzystaniem suplikanta SSL VPN GlobalProtect Palo Alto.

Zamawiający dopuszcza rozwiązania Open Source, pod warunkiem zapewnienia przez Wykonawcę wsparcia technicznego Producenta rozwiązania.

Obecnie w sieci WAN jest wdrożony system uwierzytelnienia oparty na rozwiązaniu PSK, który zapewnia w zakresie wymiany danych uwierzytelnienie urządzeń sieci WAN oraz PKI użytkowników SSL VPN zapewniających bezpieczeństwo i integralność danych oraz rozliczalność wymiany danych.

PKI zostanie wdrożona z wykorzystaniem posiadanych przez Zamawiającego zasobów opisanych w rozdziale II „Posiadana platforma sprzętowa”.

1. Wymagana funkcjonalność architektury systemu PKI:
   1. System dla PKI oparty o Urząd Certyfikacji CA, do wydawania urządzeniom i użytkownikom kluczy musi umożliwiać realizację następujących zadań:

* możliwość generowania certyfikatów dla min 500 tys. certyfikatów ,
* musi posiadać Urząd Rejestracji (RA) i Urząd Walidacji (VA),
* musi być zarządzany przez GUI WWW,
* Integracja interfejsów oraz usług dodatkowych w jednym portalu;
* automatyczne generowanie certyfikatów dla routerów (IOS,XE,XR) z wykorzystaniem protokołu SCEP,
* możliwość definiowania wielu szablonów certyfikatów,
* musi posiadać możliwość integracji z Azure AD Role Based Authentication (RBAC),
* automatyczne generowanie certyfikatów dla klienta GlobalProtect z wykorzystaniem protokołu SCEP zaterminowanego na urządzeniach PaloAlto.
* utworzenie certyfikatów routerów użytkowników na podstawie dostarczonego przez nich klucza publicznego lub klucza wygenerowanego w systemie PKI,
* automatyczną ponowną certyfikację,
* klucze prywatne dla certyfikatów końcowych muszą mieć długość co najmniej 2048 bitów,
* wsparcie dla algorytmu SHA-2,
* eksport certyfikatów i listy CRL,
* odwołanie certyfikatów użytkowników.
* Aktywne wsparcie producenta rozwiązania na 36 miesięcy.
  1. System PKI musi realizować dla routerów Cisco (IOS, XE , XR) wydanie certyfikatów do infrastruktury sieciowej WAN. System powinien umożliwiać pracę w trybie automatycznym, nie wymagającym obecności administratora.

1. Opcjonalna funkcjonalność architektury systemu PKI:
   1. Udostępnianie on-line informacji o statusie wydanego certyfikatu za pomocą protokołu komunikacyjnego opisanego w RCF 2560, w aspekcie przekazywania informacji o bieżącym statusie danego certyfikatu, np. informacji o ważności, odwołaniu lub zawieszeniu certyfikatu.
   2. Integrację z Active Directory, LDAP oraz Cisco ISE w wersji minimum 2.9.

**Rozdział II**

**1. Szczegółowy zakres platformy sprzętowej i jej konfiguracja.**

Maszyny wirtualne będą uruchamiana na platformie sprzętowej i wizualizacyjnej vCenter 6.5 Server Architecture Zamawiającego. Zamawiający posiada niezbędne licencję dla maszyn wirtualnych Red Hat.