

Zaproszenie do złożenia oferty cenowej w celu oszacowania wartości zamówienia na „Zakup rozwiązania wspierającego infrastrukturę klucza publicznego (PKI)”

1. Z uwagi na przewidywane ogromne obciążenie i ilość przechowywanych certyfikatów, oraz krytyczność systemu dla procesów biznesowych system musi być:
 - Zdolny do pracy w trybie ultra wysokiej dostępności
 - Zdolny do pracy z min. dwóch ośrodków DC jednocześnie Podstawowe i Zapasowe centrum przetwarzania w trybie Active – Active
 - Rozwiązanie powinno mieć udokumentowane wdrożenia w dużej skali (+100 mln certyfikatów) globalnie (Zamawiający dopuszcza wdrożenia na terenie EU)
 - Musi mieć udokumentowane wdrożenia w organizacjach typu WEB TRUST, czy eIDAS
 - Wsparcie dla systemu musi być dostarczane bezpośrednio przez dostawcę rozwiązania
 - W ramach wsparcia musi istnieć gotowość do wprowadzenia modyfikacji zgodnie z potrzebami zamawiającego
 - Dostępne poprawki bezpieczeństwa
2. Z uwagi na wymagania technologiczne rozwiązanie musi spełniać następujące kryteria:
 - Obsługiwać certyfikaty w następujących formatach i standardach
 - X.509 zgodne z RFC 5280
 - PKCS#10, CRMF, SPKAC
 - PKCS#12, JKS, PEM, oraz certyfikaty przechowywane w urządzeniach zgodnych z PKCS#11
 - EN 319 412 eIDAS
 - Protokół OCSP zgodny z RFC6969 i RFC 5019
 - ICAO 9303, EAC 1.11 i EAC 2.10
 - Musi wspierać integrację przy pomocy następujących protokołów:
 - CMP
 - EST
 - SCEP
 - ACME
 - REST API
 - Web Service
 - Musi wspierać kryptografię
 - RSA
 - ECDSA
 - EdDSA
 - CNSA
 - Współpracować z urządzeniami typu HSM
 - Warstwa persystencji oparta o wysokowydajne rozwiązania bazodanowe pracujące w trybie Active-Active (Oracle RAC / MariaDB / PostgreSQL / MS SQL Server)
 - Umożliwiać w łatwy sposób budowanie i dodawanie profili certyfikatów
 - Umożliwiać wydzielanie logicznych odseparowanych instancji CA
 - Posiadać rozbudowane zarządzanie poprzez Rest API
 - W pełni implementować standardy RFC 4210 oraz RFC 6712
 - Wspierać protokoły CEP, CES

- Web GUI dla modułu RA
 - Możliwość wydzielenia roli RA
 - Musi umożliwiać budowanie automatycznych przepływów pracy dla procesu zatwierdzania certyfikatów (workflows)
 - Musi w pełni wspierać transparentność certyfikacyjną opisaną w RFC 6962
 - Musi wspierać protokół ACME zgodnie z RFC 8555
 - Musi wspierać protokołów EST zgodnie z RFC 7030
 - Musi wspierać możliwość publikowania
3. Z uwagi na używaną obecnie technologię i posiadane kompetencje w zakresie jej utrzymania i zarządzania infrastrukturą system powinien:
- Umożliwiać instalację i pracę pod kontrolą systemów operacyjnych klasy OpenSource (Linux)
 - Umożliwić uruchomienie w środowiskach skonteneryzowanych (Kubernetes)
4. Zamawiający dopuszcza oferowanie rozwiązania opartego o appliance sprzętowy.
5. Zamawiający wymaga zaoferowania wsparcia producenta na okres 36 miesięcy.