Centrum Informatyki Resortu Finansów

Załącznik nr 3 do Ogłoszenia o Wstępnych Konsultacjach Rynkowych

Ogólne założenia rozwiązania wspierającego infrastrukturę klucza publicznego (PKI).

1. Z uwagi na bardzo duże przewidywane obciążenie, dużą liczbę przechowywanych certyfikatów oraz krytyczność systemu dla procesów biznesowych, proponowane rozwiązanie musi spełniać poniższe wymagania:
    a) Praca w trybie wysokiej dostępności.
    b) Zdolność do pracy w co najmniej dwóch ośrodkach przetwarzania danych jednocześnie – podstawowe i zapasowe centrum przetwarzania w trybie Active – Active.
    c) Dostępność repozytorium wystawionych i unieważnionych certyfikatach spójna dla obu ośrodków z opcją synchronizacji w możliwie krótkim czasie.
    d) Rozwiązanie powinno mieć udokumentowane wdrożenia w dużej skali (+100 mln certyfikatów), globalnie (Zamawiający dopuszcza wdrożenia na terenie EU).
    e) Musi mieć udokumentowane wdrożenia w organizacjach typu WEB TRUST, czy eIDAS.
    f) Wsparcie dla systemu musi być dostarczane bezpośrednio przez dostawcę rozwiązania. W ramach wsparcia:
        i. musi istnieć gotowość do wprowadzenia modyfikacji zgodnie z potrzebami zamawiającego,
        ii. bezpieczeństwo kodu aplikacji musi być zapewnione poprzez możliwość inspekcji kodu źródłowego lub przedstawiony wynik audytu kodu źródłowego przeprowadzony przez niezależny zespół bezpieczeństwa,
        iii. Dostępne poprawki bezpieczeństwa w terminie nie dłuższym niż 1 h od publikacji przez producenta.
2. Z uwagi na wymagania technologiczne rozwiązanie musi spełniać następujące kryteria:
    a) 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 RFC 6960 i RFC 5019,
        - ICAO 9303, EAC 1.11 i EAC 2.10.
    b) Musi wspierać integrację przy pomocy następujących protokołów:
        - CMP,
        - EST,
        - SCEP,
        - ACME,
        - REST API,
        - Web Service.
    c) Musi wspierać kryptografię:
        - RSA,
        - ECDSA,
        - EdDSA,

- CNSA.

d) Musi posiadać możliwość zarządzania za pomocą interfejsu przeglądarkowego opartego o komunikację HTTP/HTTPs.
e) Współpracować z urządzeniami typu HSM w zakresie składowania i wykorzystywania klucza prywatnego CA,
f) Warstwa persystencji oparta o wysokowydajne rozwiązania bazodanowe pracujące w trybie Active-Active (Oracle RAC / MariaDB / PostrreSQL / MS SQL Server),
g) Umożliwiać w łatwy sposób budowanie i dodawanie profili certyfikatów,
h) Umożliwiać wydzielanie logicznych odseparowanych instancji CA,
i) Posiadać rozbudowane zarządzanie poprzez Rest API,
j) W pełni implementować standardy RFC 4210 oraz RFC 6712,
k) Wspierać protokoły CEP, CES ,
l) Web GUI dla modułu Register Authority,
m) Możliwość wydzielenia roli Rest Api,
n) Musi umożliwiać budowanie automatycznych przepływów pracy dla procesu zatwierdzania certyfikatów (workflows),
o) Musi w pełni wspierać transparentność certyfikacyjną opisaną w RFC 6962,
p) Musi wspierać protokół ACME zgodnie z RFC 8555,
q) Musi wspierać protokołów EST zgodnie z RFC 7030,

3. Z uwagi na używaną obecnie technologię i posiadane kompetencje w zakresie jej utrzymania i zarządzania infrastrukturą system powinien:
    a) Umożliwiać instalację i pracę pod kontrolą systemów operacyjnych klasy OpenSource (Linux),
    b) 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.