Załącznik nr 1 do SIWZ

znak sprawy: 32/DI/PN/2013

Opis, zakres i warunki realizacji przedmiotu zamówienia

Spis treści:

Słownik pojęć

Infrastruktura Klucza Publicznego	(ang. Public Key Infrastructure) (PKI) – w ogólności jest to zespół urządzeń, oprogramowania, ludzi, polityk oraz procedur umożliwiający tworzenie, przechowywanie, zarządzanie i rozprowadzanie cyfrowych certyfikatów.
CSIZS	Centralny System Informatyczny Zabezpieczenia Społecznego realizowany w Ministerstwie Pracy i Polityki Społecznej.
Polityka certyfikacji	Szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki bezpieczeństwa tworzenia i stosowania certyfikatów.
CA	Urząd certyfikacyjny (ang. Certification Authority) , który jest odpowiedzialny za wystawianie i unieważnianie certyfikatów klucza publicznego.
TLS/SSL	(ang. Transport Layer Security) protokół komunikacyjny zapewniający bezpieczną komunikację poprzez niezaufaną sieć. Poprzednikiem TLS był protokół SSL (ang. Secure Socket Layer).
RootCA	Główny Urząd Certyfikacji – w tym postępowaniu CA_MPiPS.
SubCA	Podrzędny Urząd Certyfikacji.
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.
API	(ang. Application Programming Interface) Interfejs programistyczny systemu informatycznego umożliwiający automatyczny dostęp do funkcji z innej aplikacji.
x.509	X.509 to standard definiujący schemat dla certyfikatów kluczy publicznych, unieważnień certyfikatów oraz certyfikatów atrybutu służących do budowania hierarchicznej struktury PKI.
CVC	(ang. Card Verifiable Certificates) Standard certyfikatów cyfrowych.
CRL	Certificate Revocation List - lista certyfikatów unieważnionych przez organ certyfikujący z różnych powodów.
OCSP	(ang. Online Certificate Status Protocol) protokół komunikacyjny umożliwiający weryfikację ważności certyfikatu.
PKCS#10	(ang. Certification Request Standard) standard opisujący format komunikatu żądania wystawienia certyfikatu klucza publicznego.
PKCS#11	(ang. Cryptographic Token Interface) API definiujące uogólniony interfejs dla tokenów (generatorów kodów). Często jest stosowany w usłudze pojedynczego logowania, kryptografii klucza publicznego i systemach pełnego szyfrowania dysku
CryptoAPI	(ang. Microsoft Cryptography API) interfejs programistyczny funkcji kryptograficznych systemu operacyjnego MS Windows.
CSP	(ang. Cryptographic Service Provider) biblioteka programistyczna implementująca interfejs MS CryptoAPI.
HSM	(ang. Hardware Security Module) urządzenie przeznaczone do bezpiecznego przechowywania kluczy cyfrowych oraz do przyspieszania operacji kryptograficznych.
HA	(ang. High Availability) właściwość systemów informatycznych zapewniająca założony poziom dostępności usług (np. poprzez odporność na awarie pojedynczych elementów).
VPN	(ang. Virtual Private Network) tunel zestawiony pomiędzy urządzeniami sieciowymi poprzez który zapewnione jest bezpieczne połączenie poprzez sieć publiczną (np. Internet).
LDAP	Protokół dostępu do usługi katalogowej (ang. Lightweight Directory Access Protocol). Serwery katalogowe są wykorzystywane do przechowywania i wydajnego udostępniania informacji rzadko zmiennych (np. struktury organizacyjne, repozytoria użytkowników).
Dokumentacja	Dokumentacja utworzona przez wykonawcę w trakcie realizacji przedmiotu zamówienia.
Oprogramowanie narzędziowe	Gotowe oprogramowanie (wraz z licencjami), które zostanie wykorzystane do zbudowania systemu uwierzytelnienia i jest jego składową.
Oprogramowanie produkcyjne	Podlegający przekazaniu Zamawiającemu, produkt realizacji przedmiotu zamówienia, zestaw nowopowstałych aplikacji i komponentów zaimplementowanych przez wykonawcę oraz zainstalowane i skonfigurowane Oprogramowanie narzędziowe. System uwierzytelnienia oraz pozostałe oprogramowanie niezbędne do jego prawidłowego funkcjonowania.

Rozdział 1. Wstęp

Przedmiotem zamówienia jest wdrożenie systemu uwierzytelnienia opracowanego na potrzeby projektu ”Emp@tia – Platforma Komunikacyjna Obszaru Zabezpieczenia Społecznego” (dalej - projekt Emp@tia) ze szczególnym uwzględnieniem produktów tego projektu, w tym produktów realizacji umowy na wykonanie Centralnego Systemu Informatycznego Zabezpieczenia Społecznego (CSIZS), oznacza to wdrożenie opracowanego systemu certyfikacji systemów informatycznych używanych w jednostkach obszaru objętego projektem oraz ich użytkowników z wykorzystaniem infrastruktury klucza publicznego (PKI).

Według stanu na dzień dzisiejszy, w obszarach objętych projektem Emp@tia, nie ma wdrożonego systemu uwierzytelnienia, który zapewniłby w zakresie realizacji procedur postępowania administracyjnego oraz w zakresie wymiany danych osobowych: uwierzytelnienie systemów zewnętrznych i ich użytkowników, integralność wymienianych danych, niezaprzeczalność i rozliczalność wymiany tych danych oraz znaczenie czasem czynności wykonywanych w ramach tych procedur.

Powyższe funkcjonalności są niezbędne do realizacji jednego z podstawowych celów procesu cyfryzacji procedur administracji publicznej w zakresie zastępowania dokumentów papierowych dokumentami elektronicznymi oraz ułatwianiu obywatelom i urzędom dostępu do informacji gromadzonych w rejestrach publicznych.

Wdrożenie systemu uwierzytelnienia w ramach projektu Emp@tia przyczyni się do zapewnienia bezpieczeństwa w zakresie wymiany informacji pomiędzy jednostkami realizującymi zadania publiczne w obszarach objęty projektem Emp@tia, tj. m.in. w obszarze Rodzina i w obszarze Zabezpieczenie Społeczne oraz pozwoli osiągnąć założone cele i rezultaty projektu Emp@tia.

PKI zostanie wdrożona z wykorzystaniem posiadanych przez Zamawiającego zasobów opisanych w rozdziale „2.2 Posiadana platforma sprzętowa i narzędziowa”.

Rozdział 2. Sytuacja aktualna

2.1. Umowa na realizację CSIZS

Aktualnie w ramach projektu Emp@tia jest m.in. realizowana umowa na wykonanie CSIZS, która znajduje się obecnie na etapie implementacji produktów, w tym m.in. Platformy Integracyjnej, której zadaniem jest zapewnienie możliwości realizacji usług wymiany informacji pomiędzy podmiotami procedur postępowania administracyjnego (osoba/urząd i urząd/urząd). Produkty powstałe w ramach tego postępowania muszą się integrować z elementami platformy integracyjnej powstałej w wyniku realizacji CSIZS.

2.2. Posiadana platforma sprzętowa i narzędziowa

Opisane powyżej środowisko przedstawia posiadaną przez Zamawiającego platformę wirtualną, która jest docelową platformą systemową do wdrożenia opracowanego systemu uwierzytelnienia.

platforma wirtualna	1) 3 serwery po 32 rdzenie i 192GB pamięci RAM + 8 serwerów po 16 rdzeni i 256GB pamięci RAM; 2) wspólna pamięć masowa o pojemności 80TB (macierz) + 60 TB (macierz) na potrzeby backupów; 3) oprogramowanie wirtualizacyjne Vmware vSphere 5.1 Enterprise Plus; 4) systemy operacyjne serwerów wirtualnych: – Windows Server 2008 R2 Datacenter Edition (na ww. 3 serwerach 32-rdzeniowych) + Windows Server 2012 Datacenter Edition (na ww. 8 serwerach 16-rdzeniowych) z możliwością downgrade do dowolnej wersji),

	– Linux Red Hat Enterprise.
urządzenie HSM	2x SafeNet Luna SA 1700 wraz z 10 licencjami klienckimi bez nToken
serwera baz danych	Oracle Database Enterprise Edition 11g z opcjami Advanced Security i Partitioning.
load balancer z terminatorem sesji TLS/SSL	2 * (F5-VPR-LTM-C2400-AC, F5-VPR-LTM-B2100, F5-ADD-VPR-VCMP-2400 (16 instancji), F5-ADD-VPRASM-C2400B)
systemu kopii zapasowych	IBM Tivoli Storage Manager

Rozdział 3. Zakres przedmiotu zamówienia

Przedmiot zamówienia obejmuje:

1. Wykonanie PKI, w tym:

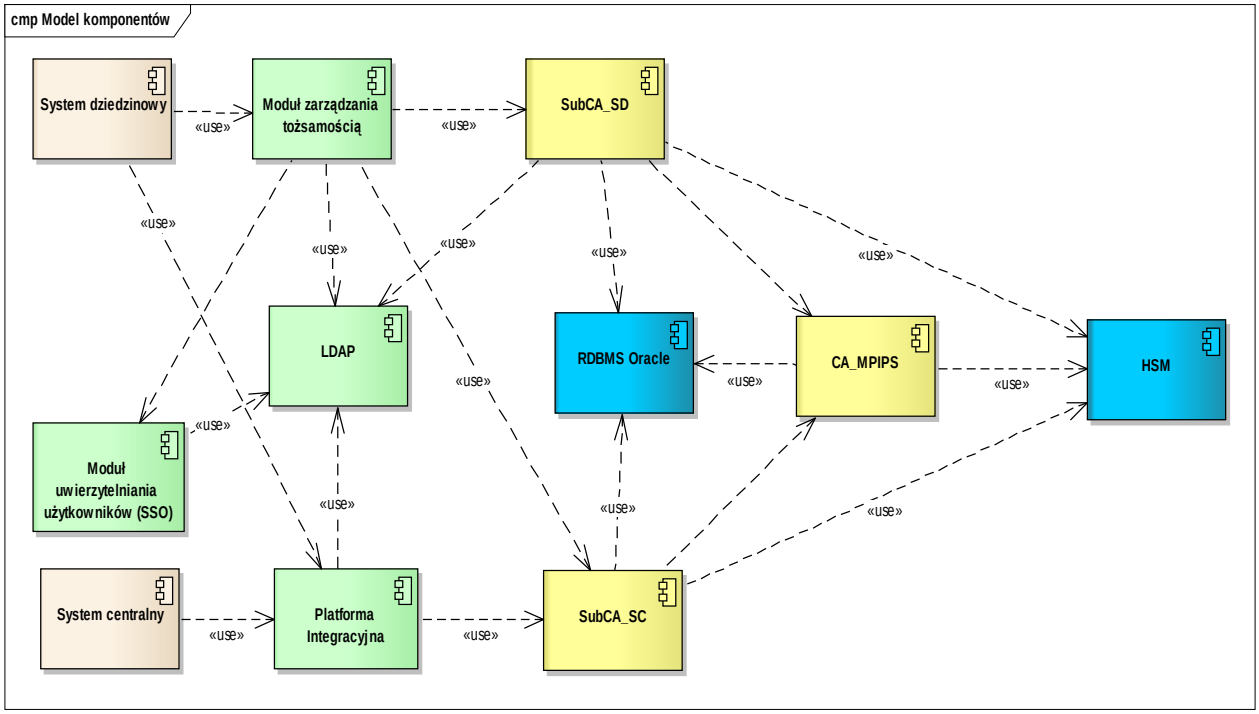
1) na podstawie analizy wymagań Zamawiającego zawartych w dokumentacji postępowania oraz dokumentacji aplikacji i systemów docelowo współpracujących z PKI wykonanie projektu funkcjonalnego i technicznego PKI, w tym uzgodnienie interfejsów PKI z systemem CSIZS,
2) dostarczenie licencji oprogramowania oraz urządzeń nie będących w posiadaniu Zamawiającego, niezbędnego do wykonania i uruchomienia środowisk PKI,
3) wytworzenie brakującego oprogramowania specjalizowanego, dedykowanego na potrzeby PKI,
4) uruchomienie oraz skonfigurowanie środowiska produkcyjnego PKI, w tym:
   a. wdrożenie i konfiguracja oprogramowania na infrastrukturze sprzętowej Zamawiającego oraz urządzeń dostarczonych w ramach Zamówienia;
   b. zasilenie inicjalne baz danych PKI;
   c. przeprowadzenie testów funkcjonalnych PKI;
   d. udział w testach integracyjnych z oprogramowaniem CSIZS;
   e. wykonanie ceremonii powołania głównego CA,
5) uruchomienie oraz skonfigurowanie środowiska testowego PKI,
6) wykonanie i przekazanie dokumentacji powykonawczej, w tym:
   a. dokumentacji instalacyjnej;
   b. instrukcji administratora;
   c. dokumentacji oprogramowania specjalizowanego, dedykowanego na potrzeby PKI;
   d. opracowanie niezbędnych polityk i procedur PKI oraz procedur eksploatacyjnych,
7) przeprowadzenie instruktażu stanowiskowego dla grupy do 10 administratorów - instruktaż zostanie przeprowadzony w siedzibie Zamawiającego.

2. Świadczenie gwarancji w okresie 1 roku od odbioru PKI, w tym: obsługa zgłoszeń awarii, wad i nieprawidłowości funkcjonowania PKI w czasie zapewniającym wymaganą dostępność, udzielanie odpowiedzi na zadane pytania, wyjaśnianie napotkanych problemów.

Elementy oprogramowania składające się na system uwierzytelnienia muszą z sobą współpracować w sposób zapewniający ergonomię użytkowania oraz bezpieczeństwo danych.

3.1. Architektura koncepcyjna

Poniższy rysunek przedstawia zakładaną architekturę koncepcyjną integracji PKI z CSIZS



Kolorem żółtym oznaczono elementy infrastruktury PKI.
Kolor zielony obrazuje oprogramowanie CSIZS.
Kolor niebieski oznacza elementy infrastruktury sprzętowej i programowej dostępne w MPiPS.

Urzędy certyfikacji (CA) przechowują klucze w HSM.

Główne CA

Główny urząd certyfikacji (CA_MPiPS) wystawia certyfikaty dla centrów podrzędnych:
- urząd do generowania certyfikatów dla systemów wewnętrznych (SubCA_SC),
- urząd do generowania certyfikatów dla systemów zewnętrznych (SubCA_SD).

Dostęp do głównego centrum certyfikacji CA_MPIPS powinien być ograniczony tylko dla upoważnionych administratorów PKI.

Centrum SubCA_SD

Centrum certyfikacji SubCA_SD powinno umożliwiać wystawienie certyfikatów dla systemów dziedzinowych (zewnętrznych):
- certyfikatów służących do podpisywania żądań zgodnie z WS Security x509 Token Profile,
- certyfikatów serwerowych SSL. Certyfikaty SSL będą służyły do uwierzytelniania systemu dziedzinowego działającego jako serwer.

Systemy dziedzinowe działają w ponad 11 tysiącach instancji (docelowo ok. 15 tys.) należących do kilku tysięcy gestorów (jednostek terenowych w obszarze Zabezpieczenie Społeczne oraz obszarze Rodzina). Systemy te są wytwarzane w różnorodnych technologiach przez kilkunastu niezależnych dostawców.

Pary kluczy i zgłoszenia certyfikacyjne zgodne z PKCS#10 są generowane przez administratora systemu dziedzinowego.

Żądania certyfikacyjne są przesyłane poprzez sieć Internet do Modułu zarządzania tożsamością będącym częścią Platformy Integracyjnej CSIZS.

Moduł zarządzania tożsamością uwierzytelnia użytkownika, który wysłał żądanie i kieruje je do centrum certyfikacji SubCA_SD. Żądanie certyfikacyjne jest żyrowane wobec SubCA_SD przez moduł zarządzania tożsamością CSIZS. Centrum SubCA_SD przyjmuje żądania tylko od modułu zarządzania tożsamością CSIZS.

Żądania certyfikacyjne są obsługiwane automatycznie w trybie synchronicznym. Wystawienie certyfikatów przez centrum SubCA_SD nie może angażować operatorów.

W komunikacji pomiędzy modułem zarządzania tożsamością a SubCA_SD preferowane jest użycie standardowych protokołów (np. SCEP, XKMS).

Certyfikaty wystawione przez SubCA_SD są przekazywane do administratorów systemów dziedzinowych za pośrednictwem modułu zarządzania tożsamością.

Certyfikaty wystawione przez SubCA_SD są rejestrowane przez moduł zarządzania tożsamością w katalogu LDAP.

SubCA_SD powinien udostępniać listę odwołanych certyfikatów CRL oraz usługę OCSP. Oba mechanizmy powinny działać w trybie wysokiej dostępności z poziomem 99%. Usługi CRL i OCSP powinny być odporne na awarie pojedynczych elementów infrastruktury.

Usługi CRL i OCSP centrum SubCA_SD powinny być dostępne w sieci Internet. Dostęp do usługi wystawiania certyfikatów powinien być ograniczony tylko dla serwerów modułu zarządzania tożsamością. Dostęp do pozostałych usług SubCA_SD powinien być możliwy tylko dla operatorów i administratorów tego centrum.

Usługi wystawiania certyfikatów SubCA_SD powinny być dostępne w trybie 24/7/365 z poziomem 90%. Czas pojedynczej niedostępności nie powinien przekroczyć 12 godzin. Okno serwisowe dopuszcza się w godzinach od 3:00 do 5:00.

Centrum SubCA_SC

Centrum certyfikacji SubCA_SC powinno umożliwiać wystawianie certyfikatów dla systemów centralnych MPiPS. Dotyczy to certyfikatów wykorzystywanych przy podpisywaniu żądań SOAP zgodnie z WS Security x509 Token Profile i XML Signature.

Certyfikaty SubCA_SC będą wystawiane na potrzeby kilkunastu systemów centralnych.

Klucze systemów centralnych są generowane przez ich administratorów za pomocą dedykowanych narzędzi (np. OpenSSL, keytool, etc).

Zgłoszenia certyfikacyjne PKCS#10 są przekazywane osobiście do operatora centrum SubCA_SC.

Certyfikat jest wystawiany przez operatora SubCA_SC.

Certyfikaty po wystawieniu są przekazywane przez operatorów do administratorów systemów centralnych.

SubCA_SC powinien udostępniać listę odwołanych certyfikatów CRL oraz usługę OCSP. Oba mechanizmy powinny działać w trybie wysokiej dostępności z poziomem 99%. Usługi CRL i OCSP powinny być odporne na awarie pojedynczych elementów infrastruktury.

Usługi CRL i OCSP centrum SubCA_SC powinny być dostępne w sieci Internet. Dostęp do pozostałych usług SubCA_SC powinien być możliwy tylko dla operatorów i administratorów tego centrum.

3.2. Wymagania wynikające z potrzeb Zamawiającego

Poniższe wymagania są obligatoryjne i muszą być spełnione w wyniku realizacji przedmiotu zamówienia.

ID	Wymaganie
	PKI
PKI.1	W ramach zamówienia konieczne jest wdrożenie dwóch środowisk PKI: 1) środowisko produkcyjne, 2) środowisko testowe. Oba środowiska powinny posiadać analogiczną konfigurację i spełniać postawione wymagania.
PKI.2	W ramach PKI musi zostać utworzony główny urząd certyfikacji CA_MPiPS, w ramach którego istnieje możliwość utworzenia hierarchii urzędów podrzędnych SubCA, w szczególności: 1) urząd do generowania certyfikatów dla systemów wewnętrznych (SubCA_SC), 2) urząd do generowania certyfikatów dla systemów zewnętrznych (SubCA_SD).
PKI.3	Urząd dla systemów wewnętrznych musi zapewnić w ramach dostarczonej licencji możliwość wydawania nielimitowanej liczby certyfikatów i rejestracji nieograniczonej liczby użytkowników.
PKI.4	Urząd dla systemów zewnętrznych musi zapewnić w ramach dostarczonej licencji możliwość wydawania nielimitowanej liczby certyfikatów i rejestracji nieograniczonej liczby użytkowników.
PKI.5	Urząd dla systemów zewnętrznych musi zapewnić w ramach dostarczonej licencji możliwość automatycznego wydawania/odnawiania nieograniczonej liczby certyfikatów poprzez interfejs API (SCEP, lub równoważny interfejs Web Service).
PKI.6	Urząd dla systemów zewnętrznych musi zapewnić możliwość wystawiania certyfikatów zgodnie z dwoma profilami: 1) serwer SSL, 2) podpisywanie danych.
PKI.7	Urząd dla systemów zewnętrznych musi umożliwiać wystawianie certyfikatów za pomocą interfejsu API z założeniem uwierzytelnienia żądań certyfikacyjnych przez aplikację – klienta usługi.
PKI.8	Musi istnieć możliwość: 1) generowania certyfikatów klucza publicznego w standardzie X.509 oraz CVC (Card Verifying Certificate), 2) generowania listy CRL/ARL, 3) weryfikacji statusu certyfikatów w oparciu o listy CRL oraz OCSP.
PKI.9	Architektura CA musi umożliwiać skalowalność rozwiązania wspieranego przez zewnętrzny system równoważonego obciążenia (load balancing). Zamawiający udostępni na potrzeby realizacji zamówienie zasoby w postaci dwóch urządzeń równoważących obciążenie sieciowe oraz terminujące sesje TLS/SSL.
PKI.10	System musi umożliwiać generowanie certyfikatów na podstawie elektronicznych wniosków w formacie PKCS#10.
PKI.11	System musi obsługiwać karty kryptograficzne z wykorzystaniem PKCS#11 lub Microsoft CryptoAPI/CSP.
PKI.12	Serwerowa część Systemu musi działać w oparciu o jeden z systemów operacyjnych:

	RedHat Enterprise Linux, Novell SuSe Linux, Microsoft Windows. Zamawiający udostępni na potrzeby realizacji Systemu licencje oprogramowania RedHat Enterprise Linux.
PKI.13	Serwerowa część systemu musi działać na bazie infrastruktury wirtualizacyjnej VMware vSphere udostępnionej przez Zamawiającego.
PKI.14	Centra certyfikacji muszą wykorzystywać urządzenie HSM zgodnego z FIPS 140-2 Level 3 do przechowywania kluczy. Zamawiający zapewni na potrzeby realizacji Systemu dostęp do urządzenia SafeNet Luna SA 1700 wraz z 10 licencjami klienckimi bez nToken.
PKI.15	System musi umożliwiać wprowadzanie polskich znaków diakrytycznych oraz będzie je poprawnie obsługiwał w generowanych certyfikatach z użyciem kodowania w standardzie UTF8.
PKI.16	Wdrażane rozwiązanie CA musi zostać uruchomione w konfiguracji o podwyższonej niezawodności (klaster aktywny-aktywny lub klaster aktywny-pasywny), które wspiera automatyczne przełączenie po awarii systemu na system rezerwowy (failover).
PKI.17	System wnioskowania o certyfikat musi umożliwić wprowadzenie minimum następujących danych: 1) Imię osoby, 2) Nazwisko osoby, 3) Identyfikator osoby (np. PESEL lub numer służbowy), 4) Nazwa organizacji, 5) Nazwa jednostki organizacyjnej (np. wydział lub departament), 6) Adres e-mail. System musi umożliwić przeglądanie i modyfikowanie rejestru oraz posiadać mechanizmy wyszukiwania rekordów z danymi spełniającymi zadane kryteria np. wyszukiwanie po nazwisku lub nazwie organizacji.
PKI.18	System musi posiadać mechanizm automatycznego powiadamiania użytkowników systemu drogą e-mailową o fakcie zbliżania się okresu końca ważności certyfikatu.
PKI.19	System musi posiadać możliwość definiowania użytkowników i przyporządkowywania im odpowiednich ról i praw dostępu a w tym przynajmniej ról: 1) Administratora, 2) Operatora, 3) Audytora.
PKI.20	System musi umożliwiać zdefiniowanie okresów zakładkowych dla list CRL.
PKI.21	System musi udostępniać możliwość odnowienia certyfikatu na te same dane.
PKI.22	System musi umożliwiać odnawianie certyfikatów bez konieczności generowania nowej pary kluczy, zawieszanie, uchylenie zawieszenia, unieważnianie certyfikatów.
PKI.23	System musi przechowywać informacje oraz certyfikaty w relacyjnej bazie danych. Dopuszczalnymi bazami danych są: DB2, Oracle, PostgreSQL, MS SQL lub MySQL. Zamawiający zapewni do celów realizacji Systemu dostęp do serwera baz danych Oracle Database Enterprise Edition 11g z opcjami Advanced Security i Partitioning.
PKI.24	Dostęp użytkowników do systemu PKI musi odbywać się z wykorzystaniem silnych technik uwierzytelniania (certyfikat na karcie kryptograficznej) – niezbędną do tego infrastrukturę zapewnia wykonawca w ramach realizacji umowy.
PKI.25	System musi wspierać okresowe i na żądanie generowanie list CRL.

PKI.26	System musi umożliwiać import, eksport oraz edycję profili certyfikatów.
PKI.27	Urzędy Certyfikacji muszą prowadzić rejestry zdarzeń umożliwiające przeprowadzenie szczegółowego audytu z pracy systemu oraz diagnostyki pracy systemu.
PKI.28	W ramach rozwiązania musi zostać dostarczone i zainstalowane oprogramowanie lub interfejs dla Punktów Rejestracji .
PKI.29	W ramach rozwiązania powinna być dostarczona funkcjonalność serwera OCSP, uruchomiona na dwóch odrębnych maszynach wirtualnych współpracujących z dwoma urządzeniami równoważącymi obciążenie (load balancing) dostarczonymi przez Zamawiającego. Serwery wirtualne OCSP będą uruchomione na dwóch różnych maszynach fizycznych. Serwer OCSP musi zapewnić możliwość obsługi 30.000 zapytań o status certyfikatu w ciągu godziny. Rozwiązanie serwerów OCSP wraz z urządzeniami balansowania ruchem musi pracować w konfiguracji HA.
PKI.30	Architektura systemu musi przewidywać utworzenie centrum zapasowego.
PKI.31	Certyfikaty wydane przez urzędy do generowania certyfikatów dla systemów muszą zawierać rozszerzenia umożliwiające pełnienie m.in. funkcji: 1) klient SSL, 2) serwer SSL, 3) urządzenia sieciowe VPN, 4) podpisywanie danych, 5) szyfrowanie danych.
PKI.32	Aplikacja CA powinna mieć możliwość automatycznej publikacji certyfikatów i list CRL do LDAP i AD. Wybór publikatora odbywa się zarówno na poziomie CA jak również profilu certyfikacji.
PKI.33	CA musi udostępniać interfejs Web Service oraz interfejs SCEP z funkcjonalnością pozwalającą na co najmniej odbieranie żądań certyfikacji, wystawianie na ich podstawie certyfikatów i odsyłanie certyfikatów do przekazującego zgłoszenie.
PKI.34	Musi istnieć możliwość zdefiniowania dla każdego CA oddzielnie, czy urząd ma wymuszać unikalność kluczy publicznych użytkowników końcowych.
PKI.35	Certyfikaty wydane przez urząd do generowania certyfikatów dla systemów wewnętrznych muszą pełnić m.in. funkcje: 1) podpisywanie danych, 2) uwierzytelnienie użytkownika, 3) klient SSL, 4) serwer SSL.
PKI.36	Dane środowisk infrastruktury PKI powinny podlegać archiwizacji z wykorzystaniem systemu kopii zapasowych IBM Tivoli Storage Manager wdrożonego w serwerowni Zamawiającego.
Gwarancja	
PKI.37	Wykonawca jest zobowiązany do świadczenia usługi gwarancji w okresie jednego roku od uruchomienia systemu PKI w zakresie pełnej funkcjonalności systemu, m.in.: poprawnego działania mechanizmów automatycznej obsługi wystawiania i unieważniania certyfikatów dla systemów, wsparcia dla użytkowników uruchomionych środowisk PKI.
PKI.38	Usługi OCSP oraz CRL powinny działać w trybie 24/7, czasy reakcji na wykryte problemy są określone w załączniku nr 3.

PKI.39	Pozostałe usługi PKI powinny działać w trybie 8/5, czasy reakcji na wykryte problemy są określone w załączniku nr 3.
	Instruktaż stanowiskowy
PKI.40	Wykonawca, w siedzibie Zamawiającego, przeprowadzi instruktaż stanowiskowy z zakresu obsługi wytworzonego systemu dla co najwyżej 10 osób wskazanych przez Zamawiającego. Wykonawca zapewni we własnym zakresie potrzebne środowisko instruktażowe - dopuszczalne jest wykorzystanie środowiska testowego. Powyższe środowisko musi być zgodne ze środowiskiem produkcyjnym w zakresie oprogramowania systemowego, bazodanowego i narzędziowego.
PKI.41	Wykonawca dostarczy wydrukowane oraz multimedialne materiały instruktażowe w postaci zapisu na płycie CD-ROM (lub innym równoważnym nośniku) zawierającego dokumenty w formacie PDF lub DOC (DOCX).
	Dokumentacja
PKI.42	W ramach zmówienia Wykonawca musi dostarczyć następującą dokumentację: **1.** Harmonogram i plan realizacji umowy, **2.** Politykę certyfikacji, **3.** Regulamin certyfikacji, **4.** Ceremonię ustanowienia urzędu CA, **5.** Analizę systemową zawierającą use case, wymagania i reguły biznesowe, **6.** Projekt Techniczny uwzględniający: 1) architekturę rozwiązania, 2) wytyczne do budowy ośrodka zapasowego, 3) model danych, 4) dokumentację użytkownika w tym instrukcję administratora, 5) specyfikację interfejsów API. **7.** Plan Testów Akceptacyjnych zawierający: 1) opis i listę scenariuszy, 2) terminy testów akceptacyjnych, 3) kategoryzację błędów i warunki odbioru, 4) opisy ról oraz odpowiedzialności osób zaangażowanych w przeprowadzenie testów, 5) sposób przeprowadzenia kolejnych iteracji testów po naprawie błędów, 6) opis środowiska testowego, 7) podejście do testowania, 8) scenariusze i przypadki testowe. **8.** Macierz pokrycia wymagań biznesowych w analizie systemowej, projekcie technicznym oraz przypadkach testowych, **9.** Raport Wyników Testów zawierający: 1) informacje o zakresie przeprowadzonych testów, 2) liczbę i rodzaj zgłoszonych błędów, 3) podsumowanie wyników testów. **10.** Plan przeprowadzenia instruktażu zawierający co najmniej szczegółowy zakres. **11.** Dokumentację eksploatacyjną, zawierającą co najmniej plan utrzymania ciągłości działania ora procedury: administracyjne, backupu systemu i danych, awaryjne, użytkownika, m.in.: 1) procedury związane z administracją i eksploatacją systemu, 2) procedury działania administratora systemu, 3) procedury awaryjne,

	4) procedury zabezpieczeń (backup'owe).
PKI.43	Dokumenty Polityki i Regulaminu certyfikacji muszą być przygotowane zgodnie z wytycznymi RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. Dla każdego CA zostanie przygotowana odrębna Polityka i Regulamin certyfikacji.
PKI.44	Cała dokumentacja, o której mowa powyżej, będzie podlegała akceptacji Zamawiającego, a także musi zostać dostarczona zgodnie z zapisami w rozdz. 4.

Rozdział 4. Realizacja przedmiotu zamówienia

Wykonawca wykona instalację i konfigurację dostarczonego Oprogramowania narzędziowego na posiadanym przez Zamawiającego środowisku opisanym w rozdziale **„2.2 Posiadana platforma sprzętowa i narzędziowa"**, a także przekaże Zamawiającemu polskojęzyczną instrukcję administratora zawierającą opis wszelkich procedur administracyjnych związanych z dostarczonym Oprogramowaniem narzędziowym.

Dostarczone licencje na Oprogramowanie narzędziowe muszą być udzielone na czas nieograniczony. Wykonawca jest obowiązany dostarczyć wszystkie licencje Oprogramowania narzędziowego niezbędne do prawidłowego działania wdrożonego systemu uwierzytelnienia, **z wyjątkiem licencji wymienionych w tabeli z rozdziału „2.2 Posiadana platforma sprzętowa i narzędziowa", udostępnianych przez Zamawiającego na potrzeby realizacji przedmiotu zamówienia.**

Każdy dokument podlegający uzgodnieniom wytworzony w ramach realizacji przedmiotu zamówienia musi być opracowany w języku polskim i dostarczony w formie:

a) wydruku (jeden egzemplarz uzgodnionej wersji dokumentu),
b) elektronicznej w formacie pdf (dla uzgodnionej wersji dokumentu),
c) elektronicznej w wersji edytowalnej (doc/docx, rtf, odt).

Ponadto dokument musi być strukturalizowany poprzez podział, co najmniej na rozdziały i podrozdziały, w taki sposób, aby umożliwiał łatwe wyszukiwanie fragmentów odnoszących się do poszczególnych poddziedzin, które wskaże Zamawiający.