(153727)

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostawa licencji EJBCA Enterprise lub równoważnych (zwanych dalej „Oprogramowaniem").

1. **Termin realizacji zamówienia:**
   Do 60 dni kalendarzowych od dnia podpisania umowy.

2. **Zamówienie obejmuje:**
   2.1. Dostawę licencji wieczystych Oprogramowania EJBCA Enterprise wraz z gwarancją i wsparciem technicznym producenta przez okres 36 miesięcy lub równoważnych, obejmujące środowiska Zamawiającego.
   Środowiska składają się z:
   - 4 serwerów CA na środowisku produkcyjnym;
   - 4 serwerów VA na środowisku produkcyjnym;
   - 12 serwerów CA na środowisku testowym;
   - 12 serwerów VA na środowisku testowym

   z zainstalowanym oprogramowaniem EJBCA Community oraz są zintegrowane z urządzeniami HSM nShield Connect XC Base.
   Dostarczone licencje nie mogą posiadać ograniczeń odnośnie liczby użytkowników, czy też liczby generowanych certyfikatów, przydzielonych vCPU lub ilością pamięci RAM na serwerze. Licencje muszą zostać dostarczone w formie elektronicznej na adres email Zamawiającego: administrator@cez.gov.pl
   2.2. Wdrożenie Oprogramowania na środowiska Zamawiającego.
   Poprzez wdrożenie Zamawiający rozumie:
   - Uzgodnienie z Zamawiającym docelowej architektury;
   - Przygotowanie planu wdrożenia;
   - Przygotowanie instrukcji instalacji i konfiguracji dostarczonego oprogramowania na środowiskach Zamawiającego wymienionych w pkt. 2.1 zgodnie z uwzględnieniem SLA;
   - Wsparcie w instalacji oprogramowania;
   - Migrację danych;
   - Weryfikację poprawności instalacji, konfiguracji i migracji danych.

   2.3. Wykonanie dokumentacji powdrożeniowej obejmującej:
   - Architekturę wdrożonego rozwiązania;
   - Schemat połączeń sieciowych;
   - Instrukcje instalacji i konfiguracji dostarczonego oprogramowania;
   - Instrukcje migracji danych;
   - Procedury administracyjne;
   - Procedury wykonania kopii bezpieczeństwa.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

2.4. Gwarancję wraz ze wsparciem technicznym producenta.
- Świadczenie Usługi Asysty Technicznej dla Oprogramowania przez okres 36 miesięcy od dnia podpisania Protokołu odbioru przez Zamawiającego.
- Pakiet usług gwarancyjnych producenta obejmować będzie aktualizacje oprogramowania, uaktualnienia, poprawki krytyczne i opcjonalne, a także wsparcie w rozwiązywaniu problemów z Oprogramowaniem oraz dostęp do bazy wiedzy producenta.
- Wymagany poziom wsparcia:
  - do 4 godzin dnia roboczego dla zgłoszeń o krytycznym priorytecie;
  - do 8 godzin dnia roboczego dla zgłoszeń o wysokim priorytecie;
  - do 2 dni roboczych dla zgłoszeń o średnim priorytecie;
  - do 4 dni roboczych dla zgłoszeń o niskim priorytecie.

3. Wymagania w zakresie wdrożenia Oprogramowania na środowiska Zamawiającego.

3.1. Wykonawca zobowiązuje się do realizacji Wdrożenia w terminie do 60 dni kalendarzowych od dnia zawarcia Umowy.

3.2. Wykonawca w terminie do 7 dni kalendarzowych od dnia zawarcia Umowy, opracuje i przekaże do akceptacji przedstawiciela Zamawiającego plan wdrożenia.

3.3. Plan wdrożenia musi uwzględniać minimalny wpływ na działanie środowiska produkcyjnego Zamawiającego.

3.4. Plan wdrożenia musi uwzględniać ewentualne kroki związane z powrotem do wersji pierwotnej (rollback).

3.5. Migracja z systemu Zamawiającego nastąpi w sposób opisany w planie wdrożenia. Wszystkie prace będą realizowane przez Zamawiającego przy wsparciu Wykonawcy.

3.6. W zakres migracji wchodzą:
- Definicje modułów kryptograficznych;
- Nadrzędne oraz podrzędne urzędy certyfikacji;
- Profile certyfikatów urzędów certyfikacji wraz z wystawionymi z nich certyfikatami;
- Profile użytkowników końcowych wraz z kontami użytkowników;
- Logi audytu;
- Role oraz grupy należących do nich użytkowników;
- Listy CRL;
- Pozostałe ustawienia administracyjne potrzebne do prawidłowego działania środowisk Zamawiającego.

3.7. Wszelkie prace muszą w pierwszej kolejności zostać wykonane na środowisku testowym Zamawiającego.

4. Kryteria stosowane w celu oceny równoważności.

4.1. Wymagania funkcjonalne Oprogramowania równoważnego:

Lp.	Wymaganie
1	Dostarczone rozwiązanie musi być opisane w dokumentacji producenta i przesłane jako bezpośredni link do dokumentacji online lub załączone jako plik PDF.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

2	Dokumentacja produktu powinna być publicznie dostępna w Internecie, aby zapewnić możliwość rozpowszechniania wiedzy o produkcie. Dokumentacja musi zawierać co najmniej: • opis architektury rozwiązania; • instrukcję instalacji i konfiguracji rozwiązania na wszystkich możliwych platformach programowych (serwer aplikacyjne, systemy operacyjne itp.); • instrukcje dotyczące uruchomienia rozwiązania w trybie wysokiej dostępności; • instrukcje zarządzania wydajnością rozwiązania; • instrukcje konfiguracji mechanizmów bezpieczeństwa rozwiązania; • instrukcję dotyczącą podniesienia wersji rozwiązania; • opis i konfiguracja możliwych integracji z urządzeniami HSM i zewnętrznymi systemami; • instrukcje postępowania w przypadku wystąpienia znanych problemów informacje odnośnie zmian w poszczególnych wydaniach oprogramowania.
3	Dokumentacja API powinna być dostępna dla wszystkich interfejsów API, które mogą być używane do wykonywania działań na produkcie.
4	Muszą istnieć przykłady kodu i biblioteki integracyjne w popularnych językach programowania, co najmniej w języku Java i Python do integracji z produktem.
5	Musi istnieć możliwość ograniczenia wydawania certyfikatów na podstawie tożsamości podmiotu/typu użytkownika, który otrzyma certyfikat.
6	Możliwe źródła tożsamości i metody uwierzytelniania administratorów do Oprogramowania: Użytkownik lokalny z hasłem, lub certyfikat z kluczami.
7	Musi istnieć możliwość ograniczenia wydawania certyfikatów na podstawie treści żądania certyfikatu związanego z algorytmem klucza, długością klucza, użyciem klucza.
8	Dostarczone rozwiązanie musi wspierać następujące standardy i formaty: • X.509, PKCS#10, PKCS#12, CRMF, SPKAC, JKS, PEM, a także urządzenia zgodne z PKCS#11, • OCSP, EAC 1.11 i EAC 2.10 • algorytmy kryptograficzne RSA, ECDSA, EdDSA i CNSA • Card Verifiable Certificates (CVC), • DNS Certificate Authority Authorization (CAA), • eIDAS, • PSD2, • FIPS 201-2 (PIV).
9	Musi istnieć możliwość rozdzielenia obowiązków i odpowiedzialności na konkretne role użytkowników, np. rola administratora wydającego certyfikat.
10	Musi istnieć możliwość uwierzytelniania standardem OAuth
11	Musi istnieć możliwość autoryzacji korzystania z platformy PKI w oparciu o grupy w usłudze ENTRA ID.
12	Jeśli w chmurze znajdują się części platformy PKI, lokalna platforma PKI musi być w stanie funkcjonować niezależnie od nich, na przykład w przypadku zerwania komunikacji.
13	Nie może być różnicy między zamawianiem, otrzymywaniem i zarządzaniem certyfikatami, gdy odbywa się to na platformie PKI w chmurze lub lokalnie.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

14	Musi istnieć możliwość generowania i ochrony kluczy prywatnych RootCA Klienta w rozwiązaniu HSM (Hardware Security Module). Przed użyciem kluczy prywatnych RootCA do podpisywania należy przeprowadzić uwierzytelnianie w rozwiązaniu HSM.
15	Musi być możliwe wygenerowanie RootCA, który nie ma klucza prywatnego przechowywanego w HSM (Hardware Security Module).
16	Komponenty PKI działające w chmurze muszą pozwalać na korzystanie z usług platformy chmurowej związanych z PKI. Na przykład HSM (Hardware Security Module) w chmurze.
17	Platforma PKI musi posiadać graficzny interfejs użytkownika, który umożliwia zarządzanie certyfikatami, nadawanie uprawnień i administrowanie Oprogramowaniem.
18	Platforma PKI musi posiadać interfejs REST API, który zapewnia opcje zarządzania certyfikatami, przyznawania uprawnień i administrowania Oprogramowaniem.
19	Platforma PKI musi posiadać możliwość powołania wielu instancji wystawiających certyfikaty, ale z indywidualnymi różnicami związanymi z wydanymi certyfikatami: • użycie kluczy, • wymagania dotyczące typu i długości klucza, • żywotność i algorytm szyfrowania.
20	Oprogramowanie musi posiadać możliwość posiadania wielu RootCA na tej samej platformie PKI.
21	Oprogramowanie musi posiadać możliwość uruchomienia wielu instancji certyfikacji w tym samym środowisku wykonawczym (maszyna wirtualna/ urządzenie/ kontener).
22	Oprogramowanie musi posiadać możliwość automatyzacji wydawania certyfikatów.
23	Podczas wydawania certyfikatu musi istnieć możliwość określenia specjalnych atrybutów i rozszerzeń, w tym pól SAN (Subject Alternate Name).
24	Musi istnieć wsparcie dla wdrażania certyfikatów z EST (Enrollment over Secure Transport).
25	Musi istnieć wsparcie dla wdrażania certyfikatów za pomocą REST API.
26	Musi istnieć wsparcie dla wdrażania certyfikatów z ACME (Automatic Certificate Management Environment).
27	Listy CRL muszą być wydawane i publikowane automatycznie dla instancji certyfikacji podłączonych do sieci.
28	Musi być możliwe uruchomienie VA (Validation Authority) lokalnie i w chmurze w sposób, który pozwoli im zawierać te same informacje.
29	VA (Validation Authority) musi obsługiwać OCSP (Online Certificate Status Protocol) w celu szybszego sprawdzania statusu certyfikatów.
30	Administracja musi być możliwa za pomocą jednego interfejsu administracyjnego. Na przykład w ramach interfejsu web
31	Musi istnieć możliwość delegowania dostępu do administracji i korzystania z części Oprogramowania osobom lub grupom.
32	Musi istnieć obsługa wdrażania certyfikatów za pomocą Microsoft Auto-enrollment lub innego automatycznego wdrażania na klientach, serwerach i kontrolerach domeny Windows.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

33	Musi istnieć możliwość publikowania certyfikatów i plików CRL w Active Directory lub innych katalogach LDAP, a także musi istnieć możliwość powiązania ich z obiektami użytkowników na podstawie tożsamości odbiorcy certyfikatu.
34	Oprogramowanie musi obsługiwać usługę JAMF lub podobne usługi do wdrażania certyfikatów na komputerach Mac.
35	Wdrożenie certyfikatów do aplikacji działających na Kubernetes musi być możliwe.
36	Komunikacja między komponentami Oprogramowania powinna opierać się na połączeniach TLS, mTLS lub wykorzystywać inne techniki w celu zapewnienia szyfrowania przesyłanych informacji i zachowania integralności.
37	Oprogramowanie musi zapewniać możliwość monitoringu ciągłości pracy w celu ustalenia czy system jest dostępny i funkcjonalny w oparciu np. o status CA, status CRL, status OCSP
38	Musi istnieć obsługa monitorowania certyfikatów wydanych przez Oprogramowanie.
39	Komponenty PKI uruchomione lokalnie, w tym RootCA, CA (Certification Authority), RA (Registration Authority) i VA (Validation Authority), będą mogły generować, przechowywać i używać kluczy prywatnych przy użyciu rozwiązania HSM (Hardware Security Module).
40	Musi być możliwe spełnienie wymagań dotyczących rozdzielenia obowiązków i odpowiedzialności dla tożsamości o różnych rolach w oparciu o logi audytu
41	Musi istnieć możliwość śledzenia całej aktywności powiązanej z czasem, tożsamością i działaniem użytkownika. Aktywność musi być identyfikowalna od początku do końca i we wszystkich komponentach, które w niej uczestniczą, a także musi być widoczna w logach audytu
42	Oprogramowanie musi umożliwić przesyłanie danych logów do SIEM (Security Information and Event Management) za pomocą jednego z poniższych sposobów: • Bezpośrednia integracja z systemem SIEM • Agent na źródle dziennika Użycie Syslog, aby zrzucić pliki dziennika do odpowiedniej pamięci pośredniej. Niezbędne jest zachowanie integralności danych.
43	Oprogramowanie musi operować w trybie active-active z minimum dwóch różnych centrów danych (DC), zapewniając nieprzerwaną pracę i odporność na awarie jednego ośrodka
44	Oprogramowanie musi zapewniać możliwość monitoringu ciągłości pracy w celu ustalenia czy system jest dostępny i funkcjonalny.
45	Oprogramowanie musi posiadać brak licencyjnych ograniczeń odnośnie liczby użytkowników czy też liczby generowanych certyfikatów
46	Oprogramowanie musi umożliwiać tworzenie i dodawanie profili certyfikatów
47	Oprogramowanie musi posiadać możliwość dodania rozszerzonego zastosowania kluczy (Extended key usage)
48	Oprogramowanie musi umożliwiać obsługę min 100 mln certyfikatów

4.2. Opis interfejsów REST API dla Oprogramowania równoważnego.

W przypadku dostarczenia rozwiązania równoważnego Wykonawca zobowiązany jest do dostarczenia rozwiązania wyposażonego w interfejsy REST API zgodnie ze specyfikacją poniżej.

4.2.1.Usługa umożliwiająca uzyskanie certyfikatu przez klienta API:

URI: /v1/certificate/enrollPkcs10Certificate

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

Metoda wywołania: POST

Wymagany format żądania (json):


```
{
 "certificate_request": "MIICh...V8shQ== OR -----BEGIN CERTIFICATE REQUEST-----
\nMIICh...V8shQ==\n-----END CERTIFICATE REQUEST-----",
 "certificate_profile_name": "ENDUSER",
 "end_entity_profile_name": "ExampleEEP",
 "certificate_authority_name": "ExampleCA",
 "username": "JohnDoe",
 "password": "foo123",
 "account_binding_id": "1234567890",
 "include_chain": true,
 "email": "john.doe@example.com"
}
```


Opis parametrów wywołania:
certificate_request - żądanie podpisania certyfikatu (CSR)
certificate_profile_name – nazwa profilu certyfikatu
end_entity_profile_name – nazwa profilu użytkownika końcowego
certificate_authority_name – nazwa urzędu certyfikacji
username – nazwa użytkownika
password – hasło
account_binding_id – identyfikator powiązanego konta
include_chain – czy zawierać łańcuch certyfikatu
email – adres e-mail

Wymagany format odpowiedzi(json):


```
{
 "certificate": "MIIDXzCCA...eW1Zro0=",
 "serial_number": "1234567890ABCDEF",
 "response_format": "DER",
 "certificate_chain": [
  "ABC123efg...345xyz0="
 ],
 "certificate_profile": "ENDUSER",
 "end_entity_profile": "ExampleEEP"
}
```


Opis parametrów odpowiedzi

certificate – wystawiony certyfikat
serial_number – numer seryjny certyfikatu
response_format – format certyfikatu
certificate_chain – łańcuch certyfikatu
certificate_profile – profil certyfikatu
end_entity_profile – profil użytkownika końcowego

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

4.2.2.Usługa umożliwiająca odwołanie certyfikatu:

URI: /v1/certificate/{issuer_dn}/{certificate_serial_number}/revoke
Metoda wywołania: PUT
Opis parametrów wywołania:
Wymagane: issuer_dn – wystawca certyfikatu certificate_serial_number – numer seryjny certyfikatu Opcjonalne: reason – powód odwołania certyfikatu – musi być zgodny z RFC5280 (jeden z: NOT_REVOKED, UNSPECIFIED ,KEY_COMPROMISE, CA_COMPROMISE, AFFILIATION_CHANGED, SUPERSEDED, CESSATION_OF_OPERATION, CERTIFICATE_HOLD, REMOVE_FROM_CRL, PRIVILEGES_WITHDRAWN, AA_COMPROMISE) Date – data odwołania certyfikatu invalidity_date – data unieważnienia certyfikatu
Wymagany format odpowiedzi(json):

status code 200
{
"issuer_dn": "CN=ExampleCA",
"serial_number": "1234567890ABCDEF",
"revocation_reason": "KEY_COMPROMISE",
"revocation_date": "1970-01-01T00:00:00Z",
"invalidity_date": "1970-01-01T00:00:00Z",
"message": "Successfully revoked",
"revoked": true
}

Opis parametrów odpowiedzi:
issuer_dn – atrybuty wystawcy certyfikatu serial_number- numer seryjny certyfikatu revocation_reason - powód odwołania certyfikatu revocation_date – data odwołania certyfikatu invalidity_date – data unieważnienia certyfikatu message – wiadomość zwrotna revoked – czy unieważniony

4.2.3.Usługa pozwalająca na pobranie listy certyfikatów danego użytkownika:

URI: /v1/certificate/search
Metoda wywołania: POST
Wymagany format żądania (json):

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

<table>
<tr><td><pre>{
 "max_number_of_results": 10,
 "criteria": [
  {
   "property": "CERTIFICATE_PROFILE",
   "value": "ENDUSER",
   "operation": "EQUAL"
  }
 ]
}</pre></td></tr>
<tr><td>Opis parametrów wywołania:</td></tr>
<tr><td>max_number_of_results – maksymalna liczba zwróconych wyników
property – właściwość
value – wartość
operation – nazwa operacji</td></tr>
<tr><td></td></tr>
<tr><td>Wymagany format odpowiedzi(json):</td></tr>
<tr><td><pre>{
 "certificates": [
  {
   "certificate": "MIIDXzCCA...eW1Zro0=",
   "serial_number": "1234567890ABCDEF",
   "response_format": "DER",
   "certificate_chain": [
    "ABC123efg...345xyz0="
   ],
   "certificate_profile": "ENDUSER",
   "end_entity_profile": "ExampleEEP"
  }
 ],
 "more_results": true
}</pre></td></tr>
<tr><td>Opis parametrów odpowiedzi:</td></tr>
<tr><td>certificate - certyfikat
serial_number - numer seryjny
response_format - format certyfikatu
certificate_chain – łańcuch certyfikatu
certificate_profile – profil certyfikatu
end_entity_profile – profil użytkownika końcowego
more_results – czy istnieje więcej certyfikatów</td></tr>
</table>

4.2.4.Usługa pozwalająca na weryfikację statusu certyfikatu:

URI: /v2/certificate/search
Metoda wywołania: POST
Wymagany format żądania (json):

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

```
{
 "pagination": {
  "page_size": 10,
  "current_page": 1
 },
 "sort": {
  "property": "USERNAME",
  "operation": "ASC"
 },
 "criteria": [
  {
   "property": "CERTIFICATE_PROFILE",
   "value": "ENDUSER",
   "operation": "EQUAL"
  }
 ]
}
```


Opis parametrów żądania:

pagination – stronicowanie
page_size – rozmiar strony
current_page – obecna strona

sort – sortuj
property – właściwość sortowania
operation – rodzaj operacji sortowania

criteria – kryteria wyszukiwania
property – właściwość wyszukiwania
value – wartość wyszukiwania
operation – nazwa operacji wyszukiwania

Opis parametrów odpowiedzi:


```
{
 "certificates": [
  {
   "fingerprint": "123abc456def789ghi123klm456nop789qrs123t",
   "c_afingerprint": "abc123def456ghi789klm123nop456qrs789tvx1",
   "certificate_profile_id": 1,
   "end_entity_profile_id": 1,
   "expire_date": 2147483647000,
   "issuer_dn": "CN=ExampleCA",
   "not_before": 1659952800011,
   "revocation_date": -1,
   "revocation_reason": -1,
   "serial_number": "1234567890ABCDEF",
   "status": 20,
   "subject_alt_name": "rfc822Name=john.doe@example.com",
   "subject_dn": "CN=John Doe,SURNAME=Doe,GIVENNAME=John,C=SE",
```


Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

```
    "subject_key_id": "z123abc456def789ghi123klm456nop789qrs123",
    "tag": "string",
    "type": 0,
    "udpate_time": 1659967133000,
    "username": "JohnDoe",
    "base64_cert": "TUlJR...t2A==",
    "certificate_request": "-----BEGIN CERTIFICATE REQUEST-----\nMIICh...V8shQ==\n---
--END CERTIFICATE REQUEST-----",
    "crl_partition_index": 1,
    "invalidity_date": -1,
    "certificate_profile": "ENDUSER",
    "end_entity_profile": "EMPTY"
   }
  ],
  "pagination_summary": {
   "page_size": 0,
   "current_page": 0,
   "total_certs": 0
  }
}
```


certificates - certyfikaty
fingerprint – odcisk palca certyfikatu
c_afingerprint – odcisk palca certyfikatu urzędu certyfikacji
certificate_profile_id – identyfikator profilu certyfikatu
end_entity_profile_id – identyfikator profilu użytkownika końcowego
expire_date – data wygaśnięcia certyfikatu
issuer_dn – atrybuty wystawcy certyfikatu
not_before – data początku ważności certyfikatuy
revocation_date – data odwołania certyfikatu
revocation_reason – powód odwołania certyfikatu
serial_number – numer seryjny certyfikatu
status – status certyfikatu
subject_alt_name – alternatywne atrybuty certyfikatu
subject_dn – atrybuty certyfikatu
subject_key_id – identyfikator klucza
tag -tag
type – typ
udpate_time – data aktualizacji
username – nazwa użytkownika
base64_cert – certyfikat zakodowany w Base64
certificate_request – żądanie podpisania certyfikatu
crl_partition_index – numer indeksu listy CRL
invalidity_date – data unieważnienia
certificate_profile – profil certyfikatu
end_entity_profile – profil użytkownika końcowego

pagination_summary – podsumowanie stronicowania

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską

page_size – rozmiar strony current_page – obecna strona total_certs – całkowika liczba certyfikatów

4.2.5.Usługa zwracająca liczbę wystawionych certyfikatów:

URI: /v2/certificate/count
Metoda wywołania: GET
Opis parametrów wywołania:
Opcjonalne: isActive – czy ma zwrócić liczbę jedynie aktywnych certyfikatów
Wymagany format odpowiedzi(json):

status code 200
{
"count": 1054
}

Opis parametrów odpowiedzi:
count - liczba certyfikatów

4.2.6.Usługa zwracająca ostatnią listę odwołanych certyfikatów (CRL):

URI: /v1/ca/{issuer_dn}/getLatestCrl
Metoda wywołania: GET
Opis parametrów wywołania:
Wymagane: issuer_dn: wystawca certyfikatów Opcjonalne: deltaCrl – czy zwrócić listę przyrostową crlPartitionIndex – index partycji listy CRL
Wymagany format odpowiedzi(json):

{
"crl": "MIIEV...SqQPE",
"response_format": "DER"
}

Opis parametrów odpowiedzi:
crl – lista CRL response_format – format listy CRL

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

4.3. Opis interfejsów SOAP API dla Oprogramowania równoważnego.
W przypadku dostarczenia rozwiązania równoważnego Wykonawca zobowiązany jest do dostarczenia rozwiązania wyposażonego w interfejsy SOAP API zgodnie ze specyfikacją zamieszczoną na stronie: https://docs.keyfactor.com/ejbca/8.3.2/web-service-interface#id-(8.3.2)WebServiceInterface-WebServicesthroughtheRA

4.4. Wymagania niefunkcjonalne Oprogramowania równoważnego.

- Musi się integrować z obecnie użytkowanym środowiskiem Zamawiającego
- Musi być przystosowane do instalacji i pracy na infrastrukturze, na której funkcjonuje aktualnie wdrożone rozwiązanie.
- Zamawiający przez równoważność rozumie licencje wieczyste zapewniające bez dodatkowych nakładów finansowych bezkonfliktowe działanie posiadanego środowiska oraz systemów z nim zintegrowanych.
- W przypadku dostarczenia licencji równoważnych Wykonawca na własny koszt wykona dostosowanie środowiska Zamawiającego w celu implementacji nowych licencji bez wpływu na dostępność środowiska.

4.5. Wymagania dodatkowe w zakresie produktów równoważnych.

- W przypadku zaoferowania przez Wykonawcę Oprogramowania równoważnego, Wykonawca dokona wdrożenia Oprogramowania równoważnego, pod nadzorem Zamawiającego, w środowisku sprzętowo-programowym Zamawiającego, zgodnie z wymaganiami opisanymi w punkcie 3 OPZ.
- Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów używanego i współpracującego z nim oprogramowania u Zamawiającego.
- Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie Oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie Oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w jego nowszych wersjach.
- Oprogramowanie równoważne musi być dostępne w sprzedaży minimum 3 lata od czasu złożenia oferty.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

Fundusze Europejskie na Rozwój Cyfrowy
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską