Warszawa, dnia 21 kwietnia 2017 r.

BA-F-II-3710-13/17

Do Wykonawców

Dotyczy: postępowania o udzielenie zamówienia publicznego na „Dostawę i wdrożenie systemu cyfrowej rejestracji przebiegu rozpraw sądowych w sądach powszechnych".

ZMIANY TREŚCI SIWZ NR 1

Ministerstwo Sprawiedliwości, jako Zamawiający w przedmiotowym postępowaniu o udzielenie zamówienia publicznego, działając zgodnie z art. 38 ust. 4 ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (t.j. Dz. U. z 2015 r. poz. 2164 z późn. zm.), zwanej dalej „ustawą" zmienia treść Specyfikacji Istotnych Warunków Zamówienia, zwanej dalej „SIWZ" w następujący sposób:

Poz. 1
Tom II: Wzór Umowy § 14. Prawa autorskie

Dotychczasowa treść:

1. Wykonawca oświadcza, że wszelkie rozwiązania dedykowane dla potrzeb realizacji Umowy, w tym Modyfikacje i oprogramowanie będące wynikiem realizacji interfejsów programistycznych umożliwiających podłączenie Centralnej Jednostki Rejestrującej do Oprogramowania ReCourt, oraz wszelka Dokumentacja (w tym materiały szkoleniowe), stworzone w wyniku zobowiązań wynikających z Umowy, stanowić będą utwory w rozumieniu art. 1 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2016 r., poz. 666 ze zm.), zwane dalej „Utworami".
2. Wykonawca przenosi na Zamawiającego, z chwilą podpisania danego Protokołu odbioru nowej wersji systemu lub Protokołu Odbioru Końcowego, majątkowe prawa autorskie do Utworów, na następujących polach eksploatacji:
   1) do programów komputerowych:
      a) trwałe lub czasowe zwielokrotnianie programu komputerowego w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie;
      b) tłumaczenie, przystosowywanie, zmiany układu lub wprowadzanie jakichkolwiek innych zmian w programie komputerowym;
      c) rozpowszechnianie, w tym użyczenie lub najem, programu komputerowego lub jego kopii.
   2) Utworów innych niż programy komputerowe:
      a) w zakresie utrwalania i zwielokrotniania Utworów - wytwarzanie określoną techniką egzemplarzy Utworów, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową;
      b) w zakresie obrotu oryginałem albo egzemplarzami, na których Utwory utrwalono - wprowadzanie do obrotu, użyczenie lub najem oryginału albo egzemplarzy;
      c) w zakresie rozpowszechniania Utworów w sposób inny niż określony w lit. b - publiczne wykonanie, wystawienie, wyświetlenie, odtworzenie oraz nadawanie i reemitowanie, a także publiczne udostępnianie Utworów w taki sposób, aby każdy mógł mieć do nich dostęp w miejscu i w czasie przez siebie wybranym,
      d) digitalizacja Utworów.
3. Z chwilą podpisania danego Protokołu odbioru nowej wersji systemu lub Protokołu Odbioru Końcowego Wykonawca przenosi na Zamawiającego prawo do wykonywania zależnego prawa autorskiego i prawa wyłącznego zezwalania na wykonywanie zależnego prawa autorskiego do Utworów, w tym prawo do rozporządzania i korzystania z opracowań Utworów, na polach eksploatacji określonych w ust. 2.
4. Wykonawca zobowiązuje się zapewnić, że osoby, którym przysługują osobiste prawa autorskie do Utworów, nie będą wykonywać swoich praw w sposób uniemożliwiający wykorzystywania praw do

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa

nich przez Zamawiającego.

5. Wykonawca oświadcza i gwarantuje, iż:
   1) najpóźniej do chwili przekazania Utworów będą mu przysługiwały wszelkie autorskie prawa majątkowe i prawa zależne do Utworów, o których mowa w niniejszym paragrafie,
   2) Utwory, ani korzystanie z tych Utworów przez Zamawiającego, nie będzie naruszać praw własności intelektualnej osób trzecich, w tym praw autorskich oraz patentów;
   3) prawa autorskie i prawa zależne określone w ust. 2 i 3 nie są i nie będą w żaden sposób ograniczone,
   4) Utwory lub utwory, z których Wykonawca skorzysta do wykonania Przedmiotu Umowy, nie będą posiadały wad fizycznych lub prawnych,
   5) rozporządzanie Utworami lub przeniesienie/zapewnienie licencji na rzecz Zamawiającego nie będzie naruszało własności przemysłowej i intelektualnej.
6. W przypadku, gdy wskutek wystąpienia w stosunku do Zamawiającego z roszczeniami zgłaszanymi przez osoby trzecie z tytułu naruszenia ich praw w związku z pracami zrealizowanymi przez Wykonawcę lub wytworzonymi przez Wykonawcę Utworami lub oprogramowaniem, programami komputerowymi lub aplikacjami wykorzystanymi przez Wykonawcę, Zamawiający nie będzie mógł korzystać z Utworów, Wykonawca niezwłocznie na swój koszt i ryzyko:
   1) dostosuje Utwory lub dostarczy nowe programy komputerowe, Dokumentację lub inne utwory albo zmieni je w taki sposób, by nie naruszały praw osób trzecich, lub
   2) uzyska dla Zamawiającego prawa określone w ust. 2 i 3 do dalszego korzystania z Utworów.

   Jeżeli postanowienia pkt 1 i 2 są niewykonalne, Zamawiający może odstąpić od Umowy.
7. W przypadku gdyby jakakolwiek osoba trzecia wystąpiła z roszczeniami wobec Zamawiającego z tytułu naruszenia jej praw, Wykonawca w szczególności:
   1) wstąpi do postępowania sądowego wszczętego przeciwko Zamawiającemu,
   2) zapewni należytą ochronę interesów Zamawiającego,
   3) zwolni Zamawiającego z wszelkich zobowiązań z tytułu naruszenia praw osób trzecich poprzez ich wykonanie lub jeżeli Zamawiający zrealizował obowiązki nałożone przez sąd lub organy administracji zwróci Zmawiającemu kwotę zapłaconych odszkodowań, kar lub innych należności,
   4) zwolni Zamawiającego od odpowiedzialności w stosunku do takich osób trzecich,
   5) zwróci Zamawiającemu wszelkie poniesione koszty związane z wystąpieniem przeciwko Zamawiającemu osób trzecich, w tym z tytułu naruszenia ich praw.
8. Wykonawca zapewnia, że korzystanie z dostarczonych Utworów podczas realizacji i na cele Umowy, w szczególności w okresie testów, nie będzie naruszać praw osób trzecich i nie będzie wymagało żadnych opłat na rzecz takich osób. Gdyby okazało się to konieczne, Wykonawca w ramach wynagrodzenia za realizację Przedmiotu Umowy udzieli lub zapewni udzielenie stosownej licencji na czas realizacji Umowy obejmującej prawo korzystania z dostarczonych rozwiązań na potrzeby realizacji Umowy do czasu uzyskania – odpowiednio – praw majątkowych lub docelowych licencji.
9. Zamawiający, z chwilą nabycia autorskich praw majątkowych i praw zależnych do Utworów, udziela Wykonawcy licencji na Utwory, na terytorium Polski, wyłącznie w celu realizacji niniejszej Umowy, na czas określony do dnia wygaśnięcia gwarancji lub rękojmi przysługującej Zamawiającemu, na następujących polach eksploatacyjnych: zwielokrotniania Utworów w całości lub w części oraz tłumaczenia, przystosowywania, zmiany układu lub wprowadzania innych zmian do Utworów.
10. Z chwilą odbioru Utworów Zamawiający nabywa własność przekazanych egzemplarzy Utworów i nośników, na których zapisano Utwory.
11. W okresie od dnia dostarczenia Utworów do momentu podpisania Protokołu Odbioru Końcowego Wykonawca udziela Zamawiającemu wyłącznej i nieograniczonej terytorialnie, z możliwością udzielania sublicencji, licencji do Utworów na polach eksploatacji określonych w ust. 2 i 3.
12. Przeniesienie praw autorskich majątkowych i praw zależnych do Utworów dokonuje się na czas nieokreślony i jest nieograniczone terytorialnie.
13. Jakiekolwiek postanowienie Umowy, w tym załączników do niej, nie ogranicza uprawnień Zamawiającego wynikających z obowiązujących przepisów prawa, w tym z art. 75 ust. 1 do 3 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych.
14. Wykonawca zobowiązuje się do nie rejestrowania jako znaków towarowych, w imieniu własnym

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa

lub na rzecz innych podmiotów, utworów graficznych lub słownych stanowiących elementy Utworów, jak też zobowiązuje się nie zgłaszać do opatentowania Utworów, co do których prawa zostaną przeniesione na Zamawiającego.

15. Do wszelkich zmian lub Modyfikacji Utworów dokonanych przez Wykonawcę w ramach gwarancji lub rękojmi albo świadczenia usług, o których mowa § 2 ust. 1 pkt 2 , stosuje się postanowienia niniejszego paragrafu, w szczególności dotyczące przeniesienia praw na Zamawiającego oraz ochrony jego praw.

Otrzymuje brzmienie:

1. Wykonawca oświadcza, iż najpóźniej w chwili przekazania Zamawiającemu oprogramowania niezbędnego do realizacji procesu rejestracji rozpraw sądowych, zarządzania nagraniami, udostępniania i przechowywania nagrań e-protokołu, Modyfikacji oraz Dokumentacji, a także innych produktów lub jakichkolwiek innych utworów, będą mu przysługiwały wszelkie autorskie prawa majątkowe i prawa zależne do utworów, o których mowa w niniejszym paragrafie,
2. Wykonawca przenosi na Zamawiającego, z chwilą podpisania danego Protokołu odbioru nowej wersji systemu lub Protokołu Odbioru Końcowego, majątkowe prawa autorskie do oprogramowania niezbędnego do realizacji procesu rejestracji rozpraw sądowych, zarządzania nagraniami (w tym nagrywania i odtwarzania), udostępniania i przechowywania nagrań e-protokołu, w tym w szczególności do wszystkich sterowników, do Modyfikacji oraz do Dokumentacji, a także do wszystkich innych produktów lub jakichkolwiek innych utworów w rozumieniu ustawy art. 1 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2016 r., poz. 666 z późn. zm.), zwanych dalej łącznie „Utworami", niezbędnych do prawidłowego działania Systemu, na następujących polach eksploatacji:
   1) do oprogramowania i programów komputerowych:
      a) trwałe lub czasowe zwielokrotnianie programu komputerowego w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie;
      b) tłumaczenie, przystosowywanie, zmiany układu lub wprowadzanie jakichkolwiek innych zmian w programie komputerowym;
      c) rozpowszechnianie, w tym użyczenie lub najem, programu komputerowego lub jego kopii.
   2) Utworów innych niż oprogramowanie i programy komputerowe:
      a) w zakresie utrwalania i zwielokrotniania Utworów - wytwarzanie określoną techniką egzemplarzy Utworów, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową;
      b) w zakresie obrotu oryginałem albo egzemplarzami, na których Utwory utrwalono - wprowadzanie do obrotu, użyczenie lub najem oryginału albo egzemplarzy;
      c) w zakresie rozpowszechniania Utworów w sposób inny niż określony w lit. b - publiczne wykonanie, wystawienie, wyświetlenie, odtworzenie oraz nadawanie i reemitowanie, a także publiczne udostępnianie Utworów w taki sposób, aby każdy mógł mieć do nich dostęp w miejscu i w czasie przez siebie wybranym,
      d) digitalizacja Utworów.
3. Z chwilą podpisania danego Protokołu odbioru nowej wersji systemu lub Protokołu Odbioru Końcowego Wykonawca przenosi na Zamawiającego prawo do wykonywania zależnego prawa autorskiego i prawa wyłącznego zezwalania na wykonywanie zależnego prawa autorskiego do Utworów, w tym prawo do rozporządzania i korzystania z opracowań Utworów, na polach eksploatacji określonych w ust. 2.
4. Wykonawca zobowiązuje się zapewnić, że osoby, którym przysługują osobiste prawa autorskie do Utworów, nie będą wykonywać swoich praw w sposób uniemożliwiający wykorzystywania praw do nich przez Zamawiającego.
5. Wykonawca oświadcza i gwarantuje, iż:
   6) Utwory, ani korzystanie z tych Utworów przez Zamawiającego, nie będzie naruszać praw własności intelektualnej osób trzecich, w tym praw autorskich oraz patentów;
   7) prawa autorskie i prawa zależne określone w ust. 2 i 3 nie są i nie będą w żaden sposób ograniczone,
   8) Utwory lub utwory, z których Wykonawca skorzysta do wykonania Przedmiotu Umowy, nie będą posiadały wad fizycznych lub prawnych,
   9) rozporządzanie Utworami lub przeniesienie/zapewnienie licencji na rzecz Zamawiającego nie będzie naruszało własności przemysłowej i intelektualnej.

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa

6. W przypadku, gdy wskutek wystąpienia w stosunku do Zamawiającego z roszczeniami zgłaszanymi przez osoby trzecie z tytułu naruszenia ich praw w związku z pracami zrealizowanymi przez Wykonawcę lub wytworzonymi przez Wykonawcę Utworami lub oprogramowaniem, programami komputerowymi lub aplikacjami wykorzystanymi przez Wykonawcę, Wykonawca niezwłocznie na swój koszt i ryzyko:
   3) dostosuje Utwory lub dostarczy nowe programy komputerowe, Dokumentację lub inne utwory albo zmieni je w taki sposób, by nie naruszały praw osób trzecich, lub
   4) uzyska dla Zamawiającego prawa określone w ust. 2 i 3 do dalszego korzystania z Utworów.

   Jeżeli postanowienia pkt 1 i 2 są niewykonalne, Zamawiający może odstąpić od Umowy.
7. W przypadku gdyby jakakolwiek osoba trzecia wystąpiła z roszczeniami wobec Zamawiającego z tytułu naruszenia jej praw, Wykonawca w szczególności:
   2) wstąpi do postępowania sądowego wszczętego przeciwko Zamawiającemu,
   3) zapewni należytą ochronę interesów Zamawiającego,
   4) zwolni Zamawiającego z wszelkich zobowiązań z tytułu naruszenia praw osób trzecich poprzez ich wykonanie lub jeżeli Zamawiający zrealizował obowiązki nałożone przez sąd lub organy administracji zwróci Zmawiającemu kwotę zapłaconych odszkodowań, kar lub innych należności,
   5) zwolni Zamawiającego od odpowiedzialności w stosunku do takich osób trzecich,
   6) zwróci Zamawiającemu wszelkie poniesione koszty związane z wystąpieniem przeciwko Zamawiającemu osób trzecich, w tym z tytułu naruszenia ich praw.
8. Wykonawca zapewnia, że korzystanie z dostarczonych Utworów podczas realizacji i na cele Umowy, w szczególności w okresie testów, nie będzie naruszać praw osób trzecich i nie będzie wymagało żadnych opłat na rzecz takich osób. Gdyby okazało się to konieczne, Wykonawca w ramach wynagrodzenia za realizację Przedmiotu Umowy udzieli lub zapewni udzielenie stosownej licencji na czas realizacji Umowy obejmującej prawo korzystania z dostarczonych rozwiązań na potrzeby realizacji Umowy do czasu uzyskania – odpowiednio – praw majątkowych lub docelowych licencji.
9. Zamawiający, z chwilą nabycia autorskich praw majątkowych i praw zależnych do Utworów, udziela Wykonawcy licencji na Utwory, na terytorium Polski, wyłącznie w celu realizacji niniejszej Umowy, na czas określony do dnia wygaśnięcia gwarancji lub rękojmi przysługującej Zamawiającemu, na następujących polach eksploatacyjnych: zwielokrotniania Utworów w całości lub w części oraz tłumaczenia, przystosowywania, zmiany układu lub wprowadzania innych zmian do Utworów.
10. Z chwilą odbioru Utworów Zamawiający nabywa własność przekazanych egzemplarzy Utworów i nośników, na których zapisano Utwory.
11. W okresie od dnia dostarczenia Utworów do momentu podpisania Protokołu Odbioru Końcowego Wykonawca udziela Zamawiającemu wyłącznej i nieograniczonej terytorialnie, z możliwością udzielania sublicencji, licencji do Utworów na polach eksploatacji określonych w ust. 2 i 3.
12. Przeniesienie praw autorskich majątkowych i praw zależnych do Utworów dokonuje się na czas nieokreślony i jest nieograniczone terytorialnie.
13. Jakiekolwiek postanowienie Umowy, w tym załączników do niej, nie ogranicza uprawnień Zamawiającego wynikających z obowiązujących przepisów prawa, w tym z art. 75 ust. 1 do 3 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych.
14. Wykonawca zobowiązuje się do nie rejestrowania jako znaków towarowych, w imieniu własnym lub na rzecz innych podmiotów, utworów graficznych lub słownych stanowiących elementy Utworów, jak też zobowiązuje się nie zgłaszać do opatentowania Utworów, co do których prawa zostaną przeniesione na Zamawiającego.
15. Do wszelkich zmian lub Modyfikacji Utworów dokonanych przez Wykonawcę w ramach gwarancji lub rękojmi albo świadczenia usług, o których mowa § 2 ust. 1 pkt 2 , stosuje się postanowienia niniejszego paragrafu, w szczególności dotyczące przeniesienia praw na Zamawiającego oraz ochrony jego praw.

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa

Poz. 2
Tom III: Opis przedmiotu zamówienia
3.1.1.7 Monitor wielkoformatowy (model B)

Dotychczasowa treść:

1.1	Wielkość ekranu: co najmniej 55”

Otrzymuje brzmienie:

1.1	Wielkość ekranu: co najmniej 54,6”

Poz. 3
Tom III: Opis przedmiotu zamówienia
3.1.1.7 Monitor wielkoformatowy (model B)

Dotychczasowa treść:

1.10	Złącza: D-SUB In, DVI-D in/out, HDMI, RS232-in/RS232-out, Display Port

Otrzymuje brzmienie:

1.10	Złącza: D-SUB In, HDMI, RS232-in/RS232-out

Poz. 4
Tom III: Opis przedmiotu zamówienia
3.4.1.1 Karty procesorowe

Dotychczasowa treść:

1.3	Wsparcie dla karty przez system zarządzania cyklem życia karty inteligentnej. Komunikacja pomiędzy kartą i systemem zarządzania odbywa się po zbudowaniu uwierzytelnionego i szyfrowanego bezpiecznego kanału pomiędzy tymi elementami.

Otrzymuje brzmienie:

1.3	Wsparcie dla karty przez system zarządzania cyklem życia karty inteligentnej. Komunikacja pomiędzy kartą i systemem zarządzania odbywa się po zbudowaniu uwierzytelnionego i szyfrowanego bezpiecznego kanału pomiędzy tymi elementami. Architektura wykorzystywanej w organizacji Zamawiającego infrastruktury klucza publicznego została opisana w Załączniku nr 1 do Opisu Przedmiotu Zamówienia „OPIS KOMPONENTÓW WCHODZĄCYCH W SKŁAD INFRASTRUKTURY KLUCZA PUBLICZNEGO BĘDĄCEJ W POSIADANIU ZAMAWIAJĄCEGO”.

Poz. 5
Tom III: Opis przedmiotu zamówienia
Do Załącznika nr 1 do Umowy - Opis przedmiotu zamówienia dodaje się Załącznik - OPIS KOMPONENTÓW WCHODZĄCYCH W SKŁAD INFRASTRUKTURY KLUCZA PUBLICZNEGO BĘDĄCEJ W POSIADANIU ZAMAWIAJĄCEGO.

Poz. 6
Tom III: Opis przedmiotu zamówienia
3.4.1.1 Karty procesorowe
Dotychczasowa treść:

1.7	Zgodność z Global Platform v2.1.1

Otrzymuje brzmienie:

1.7	Zgodność z Global Platform v2.1.1 lub równoważny, tj. Zamawiający dopuszcza w tym zakresie wykorzystanie dowolnego innego standardu, jako rozwiązanie równoważne, jeżeli zapewni ono komunikację z oprogramowaniem pośredniczącym obecnie wykorzystywanych przez Zamawiającego kart:

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa

	• Aladdin - eToken Base Cryptographic Provider • Siemens Card API CSP • Comarch SmartCard CSP

Poz. 7
Tom III: Opis przedmiotu zamówienia
3.4.1.1 Karty procesorowe
Dotychczasowa treść:

1.12	System operacyjny karty: Java Card w wersji minimum 2.2.1 lub równoważny

Otrzymuje brzmienie:

1.12	System operacyjny karty: Java Card w wersji minimum 2.2.1 lub równoważny. Za właściwy i spełniający wymaganie Zamawiającego uznany zostanie również każdy inny system operacyjny karty, który pozwoli Zamawiającemu na umieszczanie i użytkowanie na kartach posiadanych przez Zamawiającego aplikacji opracowanych w technologii Java Card wersji 2.2.1 i wyższych.

Poz. 8
Tom I: INSTRUKCJA DLA WYKONAWCÓW (IDW)
Dodaje się punkt o treści:
5.9. Zamawiający udostępni pakiet kodów źródłowych oprogramowania. W celu odebrania ww. pakietu należy zwrócić się z wnioskiem drogą elektroniczną na adres Paulina.Gecyngier@ms.gov.pl albo w formie pisemnej na adres Zamawiającego. Zamawiający niezwłocznie powiadomi o terminie i miejscu odbioru pakietu. Warunkiem odbioru pakietu będzie podpisanie zobowiązania do zachowania poufności według wzoru stanowiącego Załącznik do SIWZ.

Poz. 9
SIWZ
Do SIWZ dodaje się Załącznik - OŚWIADCZENIE DO ZACHOWANIA POUFNOŚCI.

Poz. 10
Tom I: INSTRUKCJA DLA WYKONAWCÓW (IDW)
Rozdział 18 pkt 18.1.2. ppkt 2 (lit. k)

Dotychczasowa treść:

k) Prezentacja musi być przygotowana i przeprowadzona jedynie z wykorzystaniem urządzeń dostarczonych, złożonych przez Wykonawcę na wezwanie Zamawiającego do przedstawienia Prezentacji oraz urządzeń udostępnionych przez Zamawiającego na potrzeby Prezentacji.

Otrzymuje brzmienie:

k) Prezentacja musi być przygotowana i przeprowadzona jedynie z wykorzystaniem urządzeń dostarczonych, złożonych przez Wykonawcę na wezwanie Zamawiającego do przedstawienia Prezentacji oraz urządzeń udostępnionych przez Zamawiającego na potrzeby Prezentacji oraz dowolnej (według wyboru Wykonawcy) z udostępnionych przez Zamawiającego wersji instalacyjnych oprogramowania RECourt.

Poz. 10
Tom I: INSTRUKCJA DLA WYKONAWCÓW (IDW)
Rozdział 18 pkt 18.1.2. ppkt 3 (1.7. i 1.8.)

Dotychczasowa treść:

1.7. Wykonawca zobowiązany jest do udzielania Zamawiającemu wszelkich wyjaśnień umożliwiających zbadanie, czy oferowane urządzenia posiadają wymagane cechy techniczne i funkcjonalne.
1.8. Czas trwania prezentacji nie może przekroczyć czterech godzin z wyłączeniem czasu przeznaczonego na dokonywanie ewentualnych zmian konfiguracyjnych lub naprawy błędu. W przypadku wystąpienia błędu lub konieczności wykonania zmian konfiguracyjnych Wykonawca

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa

może, celem usunięcia błędu lub dokonania zmian, poprosić o zatrzymanie czasu prezentacji. Łączny czas trwania dokonywania takich zmian lub naprawy błędów nie może przekroczyć jednej godziny. Po przekroczeniu czasu na prezentację, zadania, które nie zostały wykonane w zadanym czasie zostaną uznane za niewykonane. Ponadto po przekroczeniu czasu przeznaczonego na dokonywanie zmian konfiguracyjnych lub naprawy błędów, nie będą mogły być wykonywane żadne dalsze zmiany.
W przypadkach losowych (np. awaria zasilania, awaria sieci logicznej) czasokres usunięcia awarii nie jest wliczany do czasu prezentacji. Z tego tytułu Zamawiający zastrzega możliwość przedłużenia terminu prezentacji.

Otrzymuje brzmienie:

1.7. Wykonawca zobowiązany jest do udzielania Zamawiającemu wszelkich wyjaśnień umożliwiających zbadanie, czy oferowane urządzenia posiadają wymagane cechy techniczne i funkcjonalne (w tym prezentując odpowiednie karty urządzeń) - w przeciągu 1 godziny prezentacji.

1.8. Czas trwania prezentacji nie może przekroczyć pięciu godzin z wyłączeniem czasu przeznaczonego na dokonywanie ewentualnych zmian konfiguracyjnych lub naprawy błędu oraz wyjaśnień, o których mowa w punkcie 1.7. W przypadku wystąpienia błędu lub konieczności wykonania zmian konfiguracyjnych Wykonawca może, celem usunięcia błędu lub dokonania zmian, poprosić o zatrzymanie czasu prezentacji. Łączny czas trwania dokonywania takich zmian lub naprawy błędów nie może przekroczyć jednej godziny. Po przekroczeniu czasu na prezentację, zadania, które nie zostały wykonane w zadanym czasie zostaną uznane za niewykonane. Ponadto po przekroczeniu czasu przeznaczonego na dokonywanie zmian konfiguracyjnych lub naprawy błędów, nie będą mogły być wykonywane żadne dalsze zmiany.
W przypadkach losowych (np. awaria zasilania, awaria sieci logicznej) czasokres usunięcia awarii nie jest wliczany do czasu prezentacji. Z tego tytułu Zamawiający zastrzega możliwość przedłużenia terminu prezentacji.

Wyjaśnienia i zmiany treści SIWZ są wiążące dla Wykonawców.

DYREKTOR
Biura Administracyjno-Finansowego
Jarosław Wyżgowski

Załączniki:

1. Załącznik do Załącznika nr 1 do Umowy - Opis przedmiotu zamówienia - OPIS KOMPONENTÓW WCHODZĄCYCH
   W SKŁAD INFRASTRUKTURY KLUCZA PUBLICZNEGO BĘDĄCEJ W POSIADANIU ZAMAWIAJĄCEGO;
2. Załącznik do SIWZ - OŚWIADCZENIE DO ZACHOWANIA POUFNOŚCI.

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa

Załącznik nr 1 do Opisu Przedmiotu Zamówienia

OPIS KOMPONENTÓW WCHODZĄCYCH W SKŁAD INFRASTRUKTURY KLUCZA PUBLICZNEGO BĘDĄCEJ W POSIADANIU ZAMAWIAJĄCEGO

1. *Specyfikacja oprogramowania oraz architektury posiadanego Systemu.*

Zamawiający jest obecnie w posiadaniu oprogramowania Comarch CertificateAuthority zwanego Centrum Certyfikacji (CA), umożliwiającym pełną implementację systemu opartego o Infrastrukturę Klucza Publicznego (PKI) i pozwalającego na świadczenie usług zaufania obejmujących m.in. usługi tworzenia podpisów elektronicznych i elektronicznych znaczników czasu oraz ich walidacji, usługi związane z uwierzytelnianiem witryn internetowych, usługi OCSP, wydawanie certyfikatów zabezpieczających pocztę i kanały komunikacyjne, uwierzytelnianie i autoryzację użytkowników. W ramach struktury PKI została wprowadzona struktura urzędów certyfikacji w postaci systemu głównego urzędu certyfikacji oraz systemu podrzędnych urzędów. Wszystkie certyfikaty użytkowników są wydane z poziomu podrzędnych urzędów certyfikacji.

Zamawiający jest także w posiadaniu oprogramowania umożliwiającego podpisywanie i weryfikację wytworzonych podpisów elektronicznych (oprogramowanie SOPEL eSign - 13 300 licencji) oraz oprogramowania umożliwiającego weryfikacją wytworzonego podpisu (oprogramowanie SOPEL eVerify - licencja nieograniczona ilościowo, terytorialnie i terminowo; w ramach licencji Zamawiający ma prawo udostępniać oprogramowanie weryfikujące wytworzony podpis elektroniczny każdemu podmiotowi, który zamierza zweryfikować podpis elektroniczny wytworzony przez Zamawiającego).

Zamawiający posiada także 16 800 kart mikroprocesorowych (Comarch SmartCard 3.1) wraz z klienckim oprogramowaniem pośredniczącym pozwalających na wykorzystanie w systemie CA oraz 10 004 czytniki kart (Comarch SmartCard Reader 3.1).

Oprogramowanie Comarch CertificateAuthority składa się z czterech modułów:

1. Moduł RA (Registration Authority), który służy użytkownikowi do składania wniosków o certyfikaty,
2. Moduł RA Operator (Registration Authority Operator), który służy do akceptacji wniosków użytkowników oraz składania wniosków o zawieszenia/unieważnienie certyfikatu,
3. Moduł CA (Certificate Authority), który służy do realizacji wniosków, w tym do wystawiania certyfikatów na podstawie wniosków zaakceptowanych w RA Operator, a także do unieważniania i zawieszania wydanych certyfikatów.
4. Moduł CA Administrator (Certificate Authority Administrator), który służy do konfiguracji oprogramowania.

Wszystkie moduły systemu dostępne są z poziomu portalu webowego. Dostęp do modułów 2, 3 i 4 możliwy jest tylko w przypadku posiadania odpowiedniego certyfikatu potwierdzającego tożsamość zdalnemu komputerowi.

Oprogramowanie posiada następujące cechy oraz funkcjonalności:

1. obsługa certyfikatu w całym cyklu jego życia – od złożenia wniosku po wygaśnięcie lub unieważnienie.
2. wyszukiwanie wniosków o certyfikat według kryteriów statusu procesu certyfikacji oraz innych cech jak nazwa właściciela klucza, data złożenia wniosku,
3. odrzucanie wniosków o certyfikat,
4. zatwierdzanie wniosków o certyfikat,
5. wydawanie certyfikatu,
6. wyszukiwanie certyfikatów według kryteriów ważności (ważny, unieważniony, przeterminowany, zawieszony), nazwy właściciela klucza (CN), daty ważności certyfikatu, profilu,
7. unieważnianie certyfikatów,
8. zawieszanie certyfikatów,
9. uchylanie zawieszenia,
10. generowanie nowej listy CRL,
11. publikowanie certyfikatów w usłudze katalogowej,
12. publikowanie CRL w usłudze katalogowej,
13. udostępnianie list CRL (Certificate Revocation List) za pomocą HTTP, HTTPS oraz FTP,
14. tworzenie nowego CA (Urzędu Certyfikacji),
15. definiowanie profili certyfikatów,
16. odzyskiwanie certyfikatów wraz z kluczami,
17. możliwość stworzenia rozbudowanej infrastruktury klucza publicznego (wiele rozproszonych jednostek rejestracyjnych),
18. wydawanie certyfikatów o różnych właściwościach (w różnych profilach certyfikatów), bez konieczności wprowadzania zmian w zdefiniowanej strukturze organizacyjnej, zachowując trzystopniowy poziom dostępu i weryfikacji: Użytkownik -> Operator RA -> Operator CA.
19. współpraca ze sprzętowym modułem kryptograficznym (tzw. HSM) do przechowywania kluczy szyfrujących chroniących informacje w systemie, a niezbędnych do jego działania, wewnątrz tego modułu,
20. współpraca z kartami mikroprocesorowymi.

Struktura systemu zamawiającego jest rozproszona, tzn. każdy z 374 sądów objętych systemem posiada własną usługę katalogową. Posiadany system umożliwia korzystanie z danych użytkowników zgromadzonych na serwerach katalogowych wszystkich 374 sądów oraz uwzględnia fakt, że w Active Directory w różnych sądach mogą występować takie same nazwy użytkowników.

W zakresie wspomagania pracy administratorów oraz operatorów odpowiedzialnych za wydawanie kart, posiadane przez Zamawiającego oprogramowanie umożliwia:

1. zarządzanie zawartością kart inteligentnych na podstawie definiowania profili,

2. kilka metod wydawanie karty inteligentnej użytkownika:
    a. nadzorowana (w obecności operatora),
    b. zatwierdzana (ze wstępnym przypisaniem karty do użytkownika),
    c. samodzielna (przeprowadzona przez użytkownika).
3. Zmianę zawartości karty inteligentnej (tzw. aktualizacja profilu karty) bez konieczności przekazania karty operatorowi, przeprowadzana przez użytkownika na stacji roboczej po uprzednim wydaniu odpowiedniej dyspozycji aktualizacji profilu karty przez operatora w systemie.
4. Automatyczne tworzenie kopii zapasowych certyfikatów służących do szyfrowania danych, pozwalająca na ich odtworzenie w celu uzyskania dostępu do zaszyfrowanych danych w przypadku zgubienia lub zniszczenia karty inteligentnej. Funkcja ta nie ma zastosowanie do certyfikatów innego przeznaczenia (np. certyfikatów do podpisu cyfrowego), dla którego para kluczy została wygenerowana wewnątrz karty inteligentnej, ponieważ w takim przypadku klucz prywatny nigdy nie opuszcza bezpiecznego obszaru karty inteligentnej.
5. Definiowane przez administratora procedury określają, które z profili kart powinny być dostępne dla operatora wydającego kartę.
6. Operator ma dostęp tylko do wniosków i certyfikatów obejmujących jego jednostkę organizacyjną.
7. W przypadku wycofania karty, certyfikaty użytkownika umieszczane są na liście odwołanych certyfikatów urzędu certyfikacji CA.
8. Pełne zarządzanie zawartością karty w tym dodawanie, odnawianie, zawieszanie, wznawianie oraz unieważnianie certyfikatów PKI wydanych użytkownikowi za pomocą systemu.
9. Odblokowanie PIN do karty za pomocą procedury challenge-response (wyzwanie – odpowiedź)

W zakresie samoobsługi użytkowników posiadane oprogramowanie umożliwia dostęp do Modułu RA za pomocą portalu webowego obsługującego składanie wniosków oraz aktualizowanie zawartości karty (po uprzednim wydaniu odpowiedniej dyspozycji zmiany profilu karty przez administratora).

Inne cechy systemu:

1) Automatyczne powiadamianie o zbliżającym się terminie wygaśnięcia certyfikatów przesyłane do użytkownika oraz odpowiedniego Operatora RA.
2) Konfiguracja pozwalająca na uzyskanie wysokiej dostępności (High Availability) i równoważenie obciążenia (load balancing),
3) Współpraca z usługą katalogowa wiodących dostawców – bez konieczności rozszerzania schematu usługi katalogowej: AD 2003/2008/2012, IBM Tivoli, Novell eDir, RedHat, Siemens.

4) Współpraca z następującymi systemami operacyjnymi:
   - Microsoft Windows Server 2008 (32/64-bity) w wersji Standard, Web, Enterprise oraz Datacenter,
   - Microsoft Windows Server 2008 R2 w wersji Standard, Web, Enterprise oraz Datacenter,
   - Microsoft Windows Server 2012 R2 w wersji Standard oraz Datacenter.
5) Wspieranie następujących relacyjnych baz danych:
   - Oracle Database 10g R2
   - Oracle Database 11g
   - Microsoft SQL Server 2008 Enterprise i Standard
   - Microsoft SQL Server 2008 R2 Enterprise i Standard
   - Microsoft SQL Server 2012 Enterprise i Standard
6) Wspieranie następujących urzędów certyfikacji (CA):
   - Cybertrust® UniCERT™ with ARM,
   - Entrust ® Authority Security Manager™
   - Microsoft Windows 2003 CA SP1, R2 I SP2
   - Windows 2008 CA oraz Windows 2008 R2 CA
   - VeriSign® Managed PKI
7) Integracja ze sprzętowym modułem kryptograficznym następujących producentów:
   - Thales (nCipher)
   - SafeNet
8) Zapisywanie certyfikatów na kartach kryptograficznych Comarch SmartCard 3.1 z pomocą klienckiego oprogramowania pośredniczącego Comarch SmartCard Libraries 3.1.1 oraz obsługa kart innych producentów poprzez interfejs CSP oraz PKCS#11.
9) Generowanie raportów z możliwością eksportu do formatów minimum pdf, xlsx oraz csv:

   a. zestawienie listy użytkowników (ważnych certyfikatów) na wskazany dzień. Raport powinien zawierać przynajmniej: imię, nazwisko, sąd, datę wystawienia, datę ważności i datę unieważnienia certyfikatu, status (ważny / unieważniony / zawieszony / wygasły). Raport musi być:
      i. globalny – dostępny dla Operatora CA i obejmujący wszystkie certyfikaty
      ii. lokalny – dostępny dla Operatora RA i obejmujący jedynie certyfikaty wydane w danej jednostce organizacyjnej.
   b. lista certyfikatów użytkowników wydanych w zadanym przedziale czasu (domyślnie poprzedni miesiąc),
   c. lista certyfikatów unieważnionych w zadanym przedziale czasu (domyślnie poprzedni miesiąc),
   d. lista certyfikatów wydanych w profilu Operatorzy RA w zadanym przedziale czasu (domyślnie poprzedni miesiąc),
   e. lista certyfikatów unieważnionych w profilu Operatorzy RA w zadanym przedziale czasu (domyślnie poprzedni miesiąc).
   f. lista wniosków oczekujących na realizację z podziałem na rodzaj wniosku i profil, w którym złożono wniosek,

g. liczba użytych znaczników czasu w zadanym okresie czasu (domyślnie poprzedni miesiąc).

10) Oprogramowanie, poprzez stronę web, umożliwia składanie oraz obsługę wniosków o: nowy certyfikat, odnowienie certyfikatu, zwieszenie, uchylenie zawieszenia oraz unieważnienie certyfikatu. Zawieszenie certyfikatu nie może trwać dłużej niż 7 dni. Certyfikat, który został zawieszony, może zostać następnie unieważniony lub jego zawieszenie może zostać uchylone. Po upływie 7 dnia od momentu zawieszenia, w przypadku braku uchylenia zawieszenia, certyfikat jest automatycznie unieważniany. Jeśli w trakcie trwania zawieszenia certyfikatu następuje jego unieważnienie, to data unieważnienia certyfikatu jest datą początku zawieszenia (tj. nie może być datą końca zawieszenia).

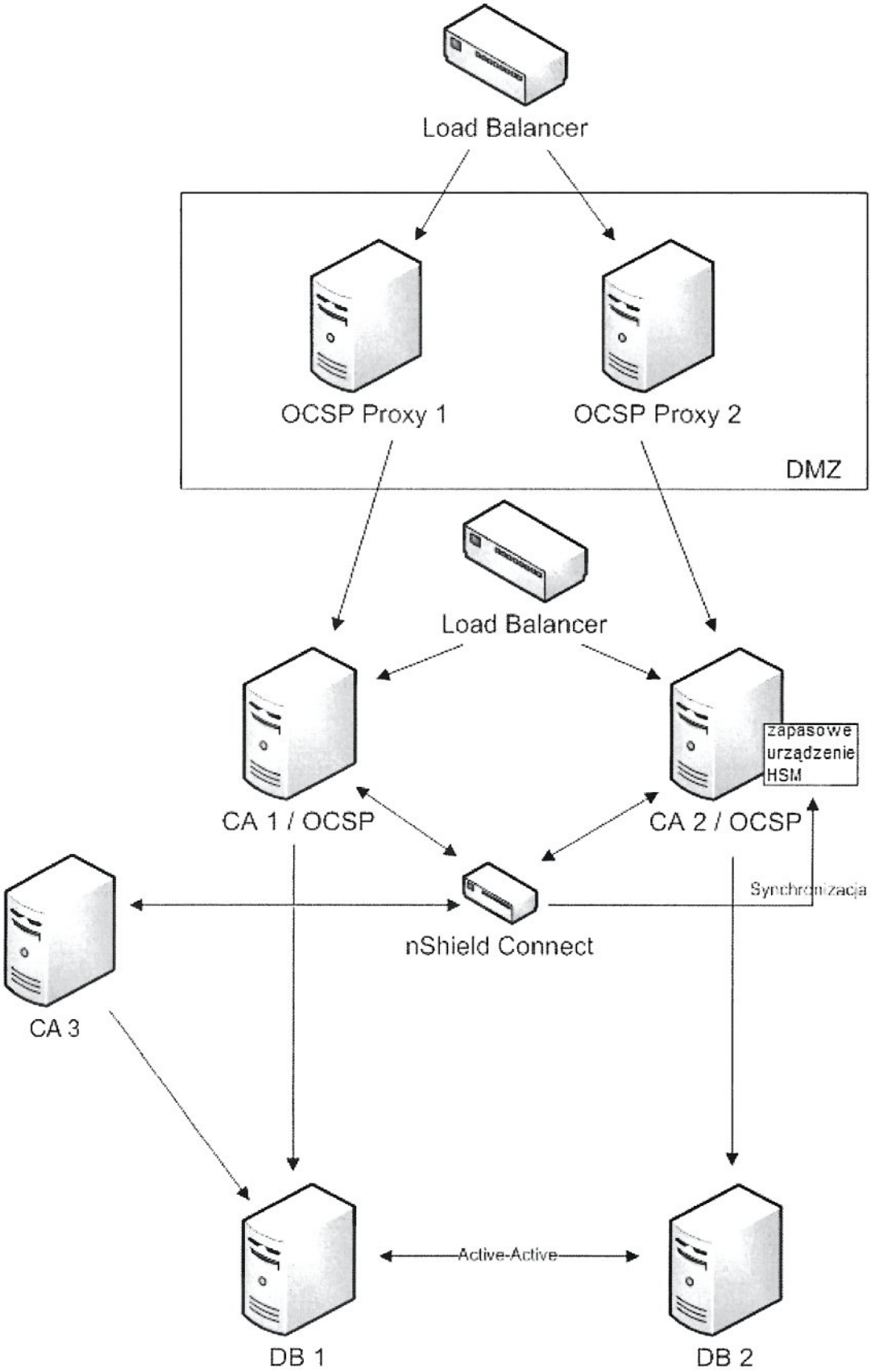
11) Współpraca z wszystkimi systemami operacyjnymi z rodziny Microsoft Windows dedykowanymi do pracy na serwerach i komputerach osobistych, począwszy od Windows XP, zarówno w wersjach 32 jaki i 64 bitowych,
12) Współpraca z przeglądarkami internetowymi:
    a. Mozilla Firefox wersja 41 i nowsze
    b. Google Chrome wersja 45 i nowsze
    c. Opera wersja 32 i nowsze
    d. Microsoft Internet Explorer 8 i nowsze
    e. Microsoft Edge wersja 20 i nowsze
13) Wsparcie dla SSL 3 oraz TLS 1.1 i TLS 1.2
14) Możliwość zatwierdzania kilku wniosków równocześnie (grupowe zatwierdzanie wniosków).
15) Możliwość otrzymywania przez Operatorów RA powiadomień e-mail o zmianie statusu wniosku oraz o zbliżającym się terminie wygaśnięcia certyfikatu
16) Personalizacja modułów systemu - możliwość dostosowania do własnych potrzeb poprzez zastosowanie na stronach web specyficznej grafiki.

W ramach aktualnie wykorzystywanego rozwiązania firmy Comarch Zamawiający posiada:

- 3 serwery firmy IBM model x3650M3 o konfiguracji: procesor Intel Xeon E5645, 16GB RAM, (dyski HDD SAS: w dwóch serwerach 4x146GB, w jednym 2x146GB) z zainstalowanym systemem operacyjnym Microsoft Windows Server 2008 R2 Standard oraz kartami nToken pozwalającymi na bezpieczną komunikację z urządzeniem HSM.
- sieciowy moduł bezpieczeństwa HSM (Hardware Security Module) nShield Connect 1500 firmy Thales.
- zapasowy HSM nShield 500e+ F3 – SEE Ready firmy Thales
- Serwer czasu rzeczywistego Elproma NTS-4000 wraz z anteną

System korzysta z bazy danych Microsoft SQL Server 2012 Standard, której dwie instancja są uruchomiana na zwirtualizowanych serwerach bazodanowych w infrastrukturze Sądu Apelacyjnego we Wrocławiu.

Architektura wdrożonego systemu przedstawiona jest na poniższym schemacie.


Load Balancer
OCSP Proxy 1
OCSP Proxy 2
DMZ
Load Balancer
CA 1 / OCSP
CA 2 / OCSP
zapasowe urządzenie HSM
Synchronizacja
nShield Connect
CA 3
Active-Active
DB 1
DB 2

Poniżej przedstawiono opis poszczególnych komponentów systemu:

1. OCSP Proxy 1

   Komponent oprogramowania OCSP (ang. Online Certificate Status Protocol) pośredniczący w komunikacji pomiędzy głównym modułem OCSP, a zewnętrznymi usługami korzystającymi z udostępnionej usługi OCSP. Komponent jest zainstalowany na udostępnionej przez Zamawiającego infrastrukturze wirtualnej. W celu zapewnienia mechanizmów wysokiej dostępności i równoważenia obciążenia oprogramowanie, poprzez Laod Balancer współpracuje z serwerem OCSP Proxy 2.
2. OCSP Proxy 2

   Komponent oprogramowania OCSP pośredniczący w komunikacji pomiędzy głównym modułem OCSP, a zewnętrznymi usługami korzystającymi z udostępnionej usługi OCSP. Komponent jest zainstalowany na udostępnionej przez Zamawiającego infrastrukturze wirtualnej. W celu zapewnienia mechanizmów wysokiej dostępności i równoważenia obciążenia oprogramowanie, poprzez Laod Balancer współpracuje z serwerem OCSP Proxy 1.
3. CA 1 / OCSP (IBM x3650M3)

   Instalacja głównego serwera CA oraz usług OCSP i znakowania czasem. Mechanizmy wysokiej dostępności i równoważenia obciążenia zostały zapewnione poprzez współpracę z serwerem CA 2 za pośrednictwem Load Balancera. Oprogramowanie zainstalowane jest na serwerze fizycznym wyposażonym w kartę nToken pozwalającą na bezpieczną komunikację z sieciowym modułem bezpieczeństwa HSM nShield Connect.
4. CA 2 / OCSP (IBM x3650M3)

   Instalacja zapasowego serwera CA oraz usług OCSP i znakowania czasem. Mechanizmy wysokiej dostępności i równoważenia obciążenia zostały zapewnione poprzez współpracę z serwerem CA 1 za pośrednictwem Load Balancera. Do serwera zostało podłączone zapasowe urządzenie HSM nShield Solo. Konfiguracja nShileld Connect 1500 dotycząca kluczy CA została powielona w urządzeniu zapasowym. W przypadku awarii głównego urządzenia HSM, serwer CA 2 / OCSP wraz z zapasowym HSM zapewni realizację wymaganej funkcjonalności. Oprogramowanie zainstalowane jest na serwerze fizycznym.
5. CA 3 (IBM x3650M3)

   Serwer fizyczny, odpowiedzialny za obsługę procedury challenge-response (wyzwanie-odpowiedź) do odblokowania PIN-u chroniącego zawartość karty kryptograficznej. Na serwerze uruchomiono środowisko testowe Systemu. Serwer komunikuje się z testową bazą danych uruchomioną na serwerze DB1. W celu zapewnienia bezpiecznej komunikacji z sieciowym modułem bezpieczeństwa HSM, serwer został wyposażony w kartę nToken.
6. DB 1

   Główna instancja bazy danych Systemu Centrum Certyfikacji. Wysoka dostępność została zapewniona poprzez mechanizm HA w trybie active-active. Baza danych została zainstalowana w architekturze wirtualnej dostarczonej przez Zamawiającego. Na serwerze uruchomiona jest także baza wykorzystywana przez środowisko testowe.
7. DB 2

Zapasowa instancja bazy danych Systemu Centrum Certyfikacji. W celu zapewnienia wysokiej dostępności usług serwer pracuje w HA w trybie active-active. Baza danych została zainstalowana w architekturze wirtualnej dostarczonej przez Zamawiającego.

8. nShield Connect

   Główne urządzenie HSM Systemu Centrum Certyfikacji. Aby zapewnić mechanizm HA, konfiguracja urządzenia dotycząca kluczy została powielona na zapasowym urządzeniu HSM, które w razie awarii głównego urządzenia zapewnia wymagane funkcjonalności.
9. Load Balancer

   Zamawiający posiada urządzenie load balancer firmy F5 Networks (z oprogramowaniem BIG-IP LTM). Urządzenie wykorzystywane jest do realizacji mechanizmów wysokiej dostępności i równoważenia obciążenia.

Na serwerach **CA1, CA2 i CA3** zainstalowane są systemy operacyjne Windows Serwer 2008 R2 Standard.
Serwery DB1 i DB2 pracują pod kontrolą systemu Windows Serwer 2012 Datacenter z systemem zarządzania bazą danych Microsoft SQL Server 2012 Standard
Na serwerach OCSP Proxy 1 i OCSP Proxy 2 zainstalowano system operacyjny CentOS 7.0

System Centrum Certyfikacji posiada także moduły OCSP oraz znakowania czasem spełniające wymagania przedstawione poniżej:

Szczegółowy opis modułu OCSP

1. Moduł OCSP realizuje protokół OCSP zgodnie ze standardem RFC 2560.
2. Moduł OCSP umożliwia obsługę wielu CCK (Centrów Certyfikacji Kluczy) w ramach jednej instalacji oprogramowania.
3. Moduł OCSP wykorzystuje bazy danych CCK jako źródła informacji o unieważnieniach.
4. Moduł OCSP synchronizuje czasu z centralnym serwerem czasu NTP.
5. Moduł OCSP współpracuje z HSM za pośrednictwem interfejsu PKCS#11 lub CSP.
6. Moduł OCSP zapewnia wydajność umożliwiającą weryfikację co najmniej 100 000 certyfikatów na godzinę.
7. Licencja modułu OCSP nie ogranicza ilości klientów, zapytań oraz generowanych odpowiedzi.

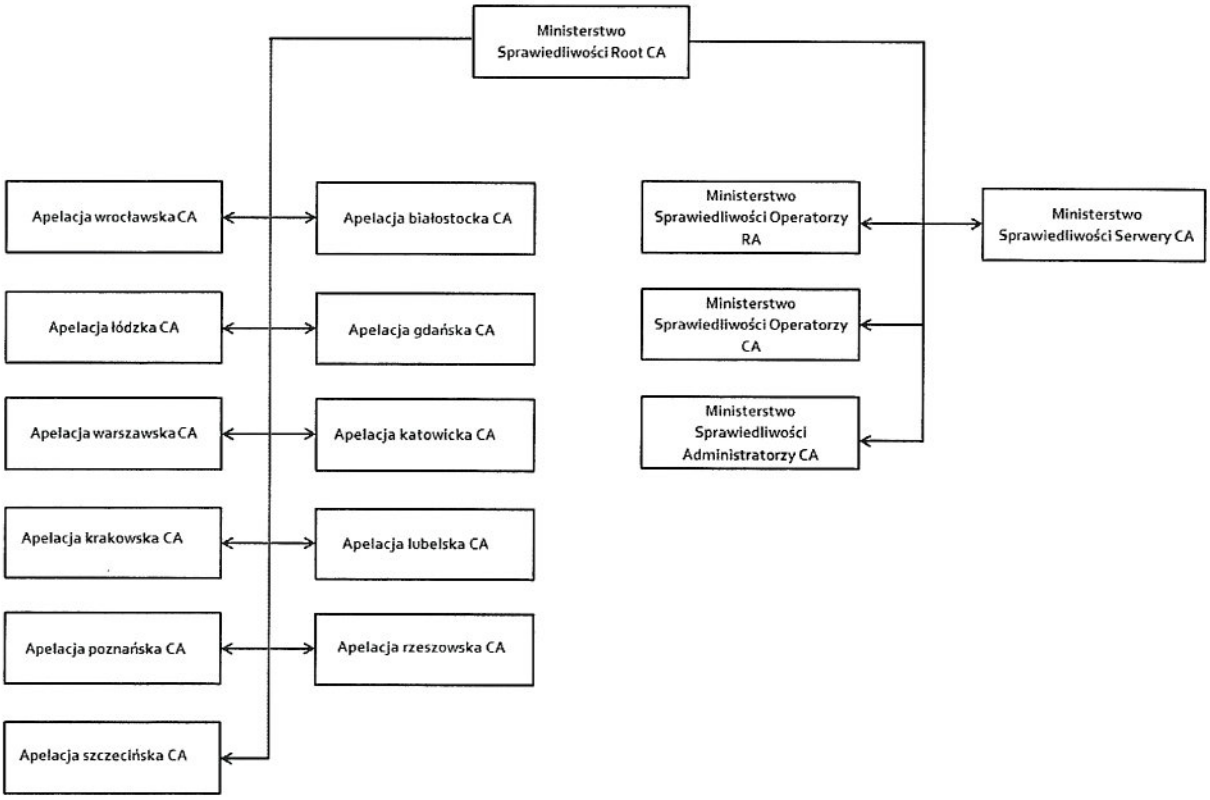
Szczegółowy opis modułu znakowania czasem

1. Moduł znakowania czasem umożliwia wystawianie znaczników czasu zgodnie ze standardem RFC 3161, korzystając z HTTPS jako protokołu transportowego.
2. Moduł znakowania czasem synchronizuje czas z centralnym serwerem czasu NTP będącym w posiadaniu Zamawiającego.
3. Moduł znakowania czasem współpracuje z HSM za pośrednictwem interfejsu PKCS#11 lub CSP.
4. Moduł znakowania czasem zapewnia wydajność umożliwiającą oznakowanie czasem 10 000 (dziesięciu tysięcy) dokumentów/komunikatów na godzinę.

5. Licencja modułu znakowania czasem nie ogranicza ilości wydawanych znaczników czasu i liczby klientów korzystających z modułu.

Komponent sprzętowy do ochrony certyfikatu oraz klucza prywatnego ma postać karty inteligentnej wraz z czytnikami w standardzie USB. Na karcie składowany jest certyfikat wraz z kluczem prywatnym, który służy do podpisywania dokumentów. Komunikacja komponentu sprzętowego z systemem operacyjnym zapewnia klienckie oprogramowanie pośredniczące wykorzystujące interfejsy CSP oraz PKCS#11.
W ramach struktury PKI wprowadzona została struktura urzędów certyfikacji w postaci systemu głównego urzędu certyfikacji oraz systemu urzędów podrzędnych. Wszystkie certyfikaty użytkowników wydane są z poziomu podrzędnych urzędów certyfikacji.

Na poniższym schemacie została przedstawiona struktura PKI:



Ministerstwo Sprawiedliwosci Root CA
Główny urząd certyfikacji, wydający certyfikaty podrzędnych CA

Ministerstwo Sprawiedliwosci Operatorzy RA
Certyfikat CA wydającego certyfikaty dla operatorów RA, umożliwiających dostęp do panelu operatora RA

Ministerstwo Sprawiedliwosci Operatorzy CA
Certyfikat CA wydającego certyfikaty dla operatorów CA, umożliwiających dostęp do panelu operatora CA

Ministerstwo Sprawiedliwosci Adminstratorzy CA
Certyfikat CA wydającego certyfikaty dla administratorów CA, umożliwiających dostęp do panelu administratora CA

Ministerstwo Sprawiedliwosci Serwery CA
Certyfikat CA wydającego certyfikaty dla serwerów www

CA Apelacji
Certyfikaty CA wydającego certyfikaty dla użytkowników w sądach z obszaru danej apelacji.

2. *Specyfikacja sieciowego moduł bezpieczeństwa HSM (ang. Hardware Security Modules) posiadanego przez Zamawiającego.*

1. Urządzenie posiada podwójne, w pełni redundantne zasilanie (2 zasilacze typu *Hot-Swap*) oraz chłodzenie w celu zapewnienia ciągłości pracy w krytycznych systemach bezpieczeństwa przedsiębiorstwa;
2. Urządzenie jest zasilane napięciem: 100-240V AC (*50-60 Hz*);
3. Urządzenie w celu przechowywania danych posiada dysk twardy typu *Solid-State;*
4. Urządzenie ma wielkość 1U i posiada możliwość montażu w szafie teleinformatycznej typu RACK 19";
5. Urządzenie posiada 2 porty Gigabit Ethernet, dodatkowo przedni panel urządzenia posiada:
   - czytnik kart pamięci (*ang. Smart Card Reader*);
   - port USB (*ang. Universal Serial Bus*);
   - diody ostrzegające o nieprawidłowym działaniu urządzenia (*ang. Warning LED*);
   - wyświetlacz typu LCD (*ang. Liquid Crystal Display*), w celu wykonania podstawowej konfiguracji oraz wyświetlania podstawowych informacji konfiguracyjnych urządzenia.
6. Waga urządzenia nie przekracza 12kg;
7. Urządzenie obsługuje następujące algorytmu szyfrowania danych:
   - RSA (1024, 2048, 4096 oraz 8192 bit);
   - Diffie-Hellman;
   - DSA;
   - El-Gamal;
   - KCDSA;
   - ECDSA;
   - ECDH;
   - AES;
   - ARIA;
   - Camellia;
   - CAST;
   - DES;
   - SEED;
   - Triple DES.
8. Urządzenie obsługuje następujące funkcje hashujące (mieszające):
   - SHA-1;
   - SHA-2 (224,256,384,512 bit);

9. Urządzenie obsługuje następujące systemy operacyjne:
   - Windows 2012 R2/2012/2008 R2/2008/2003/Vista/XP;
   - Solaris;
   - HP-UX;
   - AIX;
   - Linux.
10. Urządzenie spełnia następujące normy oraz posiada certyfikaty:
   - UL, CE, FCC;
   - FIPS 140-2 Level 2/3, NIST SP 800-131A;
   - Common Criteria EAL4+.
   - RoHS, WEEE
11. Urządzenie jest w stanie przetworzyć 1500 transakcji na sekundę. Transakcja rozumiana jest jako ilość podpisów cyfrowych wykonanych algorytmem *RSA* z kluczem 1024 bitowym;
12. Urządzenie wspiera do 20 klientów;
13. Urządzenie ma możliwość zarządzania za pomocą dwóch interfejsów: CLI (*ang. Command Line Interface*) oraz GUI (*ang. Graphical User Interface*)
14. Interfejs zarządzający ma możliwość definiowania tzw. ról użytkowników;
15. Urządzenie posiada obsługę protokołu SNMPv3;
16. Urządzenie posiada oprogramowanie, które może aktualizować do nowszych wersji;
17. Urządzenie posiada możliwość integracji z drugim takim samym urządzeniem w celu utworzenie tzw. klastra oraz funkcji „*Load-Balancing*".
18. Średni czas bezawaryjnej pracy urządzenia wynosi 47 000 godzin.

3. Specyfikacja zapasowego urządzenia HSM

1. Urządzenie pozwala na instalację w slocie PCIe.
2. Urządzenie posiada czytnik kart pamięci (*ang. Smart Card Reader*) w postaci dołączanego zewnętrznego urządzenia.
3. Urządzenie obsługuje co najmniej następujące algorytmy szyfrowania:
   - RSA (1024, 2048, 4096),
   - Diffie-Hellman,
   - DSA,
   - El-Gamal,
   - KCDSA,
   - ECDSA,
   - ECDH,
   - AES,
   - ARIA,
   - Camellia,
   - CAST,
   - DES,
   - RIPEMD160 HMAC,
   - SEED,
   - Triple DES
4. Urządzenie obsługuje następujące funkcje haszujące (mieszające):
   - SHA-1;

- SHA-2 (224, 256, 384, 512 bit)

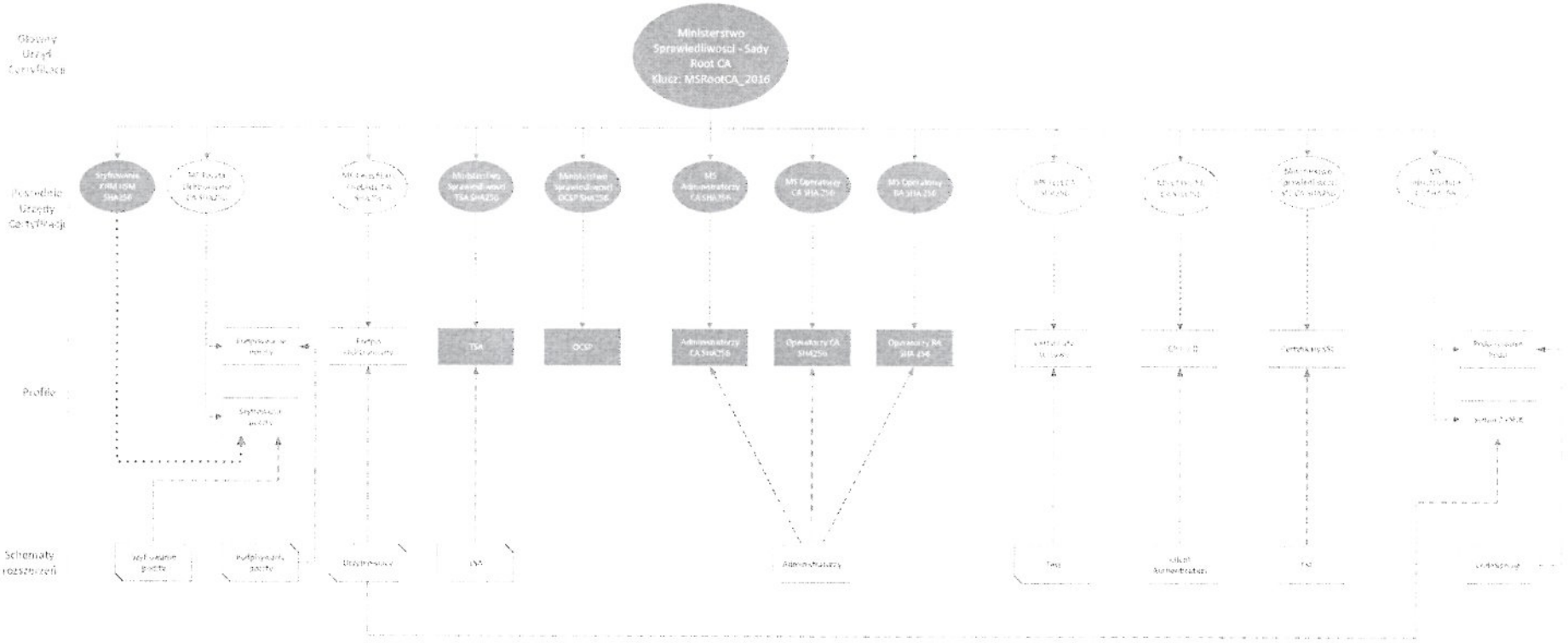
5. Urządzenie obsługuje następujące systemy operacyjne:
   - MS Windows 2012 R2/2012/2008 R2/2008/2003
   - Linux
   - Solaris
   - IBM AIX
   - HP-UX
6. Urządzenie spełnia następujące normy oraz posiada certyfikaty:
   - UL, CE, FCC
   - RoHS, WEEE
   - FIPS 140-2 Level 2/3, NIST SP 800-131A
   - Common Criteria EAL4+
7. Urządzenie przetwarza co najmniej 500 transakcji na sekundę (jako transakcję rozumie się ilość podpisów cyfrowych wykonanych algorytmem RSA z kluczem 1024 bitowym)
8. Urządzenie posiada możliwość zarządzania za pomocą dwóch interfejsów: CLI (*ang. Command Line Interface*) oraz GUI (*ang. Graphical User Interface*),
9. Interfejs zarządzający ma możliwość definiowania tzw. ról użytkowników
10. Urządzenie posiada obsługę protokołu SNMPv3
11. Urządzenie umożliwia aktualizowanie oprogramowanie do nowszych wersji,
12. Średni czas bezawaryjnej pracy urządzenia wynosi co najmniej 125 000 godzin.
13. Urządzenie współpracuje i umożliwia konfigurację mechanizmu HA z HSM nShield Connect 1500 firmy Thales.
14. Urządzenie pochodzi z oficjalnego kanału dystrybucyjnego w Unii Europejskiej.

4. Specyfikacja serwera czasu rzeczywistego

1. Sprzętowy serwer zapewniający dostarczanie jednolitego czasu zgodnie z protokołem NTP v3 lub nowszym.
2. Serwer czasu pobiera aktualny czas ze źródła czasu urzędowego w Polsce (UTC PL).
3. Serwer czasu posiada zewnętrzny odbiornik GPS i umożliwiający ustawienie źródła czasu międzynarodowego (UTC) jako czasu rezerwowego.
4. Serwer czasu posiada dokładność na poziomie nie gorszym niż 900 (dziewięćset) milisekund przy braku źródła synchronizacji czasu przez okres 1 tygodnia.
5. Serwer czasu posiada automatyczny system kontroli pracy modułu i stabilności czasu umożliwiający wysyłanie powiadomień poprzez e-mail, SNMP.
6. Serwer czasu obsługuje protokoły sieciowe TCP, UDP, IP v4, IP v6
7. Serwer czasu posiada możliwość zarządzania przy pomocy protokołu HTTPS, SSH, SNMPv3.
8. Serwer czasu posiada co najmniej dwa interfejsy sieciowe.
9. Serwer czasu umożliwia priorytetyzację źródeł czasu odniesienia.
10. Serwer czasu posiada wydajność na poziomie co najmniej 5000 (pięć tysięcy) zapytań na sekundę.

11. Serwer czasu pozwala na instalacje w szafie RACK 19" i posiada wysokość 1U.
12. Serwer czasu posiada możliwość pracy w temperaturze od 0°C do 50°C
13. Średni czas bezawaryjnej pracy urządzenia wynosi co najmniej 280 000 godzin.
14. Urządzenie zasilane jest napięciem: 110-230VAC (50-60 Hz).
15. Serwer jest wyposażony w wyświetlacz umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie urządzenia.
16. Urządzenie jest chłodzone pasywne.

Struktura CA



Załącznik do SIWZ

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

Ja niżej podpisany/a niniejszym oświadczam, że:

1) nie ujawnię bez stosownego upoważnienia wydanych przez Ministerstwo Sprawiedliwości kodów źródłowych oraz żadnych informacji w tym zakresie, w szczególności prawnie chronionych, a także o sposobach zabezpieczenia stosowanych w Ministerstwie Sprawiedliwości, o ile wejdę w ich posiadanie, oraz nie przyczynię się do ich ujawnienia lub innych działań związanych z ich przetwarzaniem lub utratą itp. mogących spowodować szkodę dla Ministerstwa Sprawiedliwości, innych osób i podmiotów lub naruszenie przepisów prawa, w tym regulacji Ministerstwa Sprawiedliwości, zarówno w trakcie wykorzystywania otrzymanych kodów źródłowych jak i po ich zakończeniu oraz będę przestrzegał/a wszelkich przepisów w tym zakresie;
2) zobowiązuję się nie wykraczać poza nadane mi uprawnienia oraz zobowiązuję się wykorzystywać przekazane mi kody źródłowe zgodnie z ww. zasadami poufności;
3) udostępnione kody źródłowe wykorzystam tylko i wyłącznie na potrzeby postępowania o udzielenie zamówienia publicznego na Dostawę i wdrożenie systemu cyfrowej rejestracji przebiegu rozpraw sądowych w sądach powszechnych, BA-F-II-3710-13/17;
4) zobowiązuję się przestrzegać oraz jestem świadomy/a odpowiedzialności za naruszenie obowiązujących zasad, wynikających w szczególności z:
   a) ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922),
   b) ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2016 r. poz. 1167),
   c) rozdziału XXXIII ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2016 r., poz. 1137 z późn. zm.).

_____ _____ _____

imię i nazwisko seria i nr dowodu osobistego/PESEL podpis

_____ _____

miejscowość data

Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa