Opis przedmiotu zamówienia ARiMR

1. **DEFINICJE**

|  |  |
| --- | --- |
| Podpis elektroniczny | kwalifikowany podpis elektroniczny na karcie kryptograficznej wraz z czytnikiem USB lub podpis zdalny - bez wymaganego czytnika i fizycznej karty kryptograficznej (QSCD zdalne - podpis zdalny)  |
| Rozporządzenie EIDAS | rozporządzenie Parlamentu Europejskiego i sRady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73). |
| PPT - Punkt Potwierdzania Tożsamości | miejsce/lokalizacja, gdzie wykonywane są czynności, polegające na bezpapierowym: weryfikowaniu tożsamości przyszłych Subskrybentów, przyjmowaniu wniosków o wydanie certyfikatów, podpisywania umów o świadczenie kwalifikowanych usług zaufania, rejestrowaniu Subskrybentów, zgłaszanie wniosków do unieważnienia certyfikatów. |

1. **PRZEDMIOT ZAMÓWIENIA**
	1. Przedmiotem zamówienia jest:
		1. świadczenie na rzecz Zamawiającego kwalifikowanych usług zaufania,
		2. udzielenie Zamawiającemu licencji uprawniającej do korzystania z oprogramowania udostępnionego przez Wykonawcę i wymaganego do świadczenia kwalifikowanych usług zaufania w okresie ich obowiązywania, umożliwiającej korzystanie z oprogramowania i obsługiwanych przez nie urządzeń zgodnie z ich charakterem i przeznaczeniem oraz warunkami Umowy i ogólnymi warunkami licencyjnymi producenta oprogramowania,
		3. dostarczenie min. 6 urządzeń mobilnych (Terminali) do wydawania podpisów elektronicznych przez pracowników Zamawiającego
	2. Świadczenie kwalifikowanych usług zaufania przez Wykonawcę obejmuje:
		1. dostarczanie i wydawanie Certyfikatów kwalifikowanych do Podpisu elektronicznego, w tym:
		2. dostarczenie nowych Certyfikatów kwalifikowanych z okresem obowiązywania 36 miesięcy każdy dla max 2400 (min. 500 szt.) Subskrybentów, zgodnie z bieżącym zapotrzebowaniem Zamawiającego zgłaszanym Wykonawcy w trakcie obowiązywania Umowy (z fizyczną kartą, oraz dodatkowo z kartą kryptograficzną wraz z programem do obsługi kart i czytnikiem USB, przy czym Zamawiający zastrzega sobie również prawo do skorzystania z opcji podpisu zdalnego - bez wymaganego czytnika i fizycznej karty kryptograficznej, w ilości min. 100 szt, QSCD zdalne);
		3. odnowienia posiadanych przez Zamawiającego certyfikatów kwalifikowanych, dla max 6.000 (min. 500 szt.) Subskrybentów, w terminach gwarantujących ciągłość posiadanych przez Subskrybentów uprawnień do Podpisu elektronicznego, poprzez przekształcenie przez Wykonawcę posiadanych na dzień zawarcia Umowy certyfikatów (dostawcą usług dla Zamawiającego przed zawarciem Umowy był Asseco Data System SA), z automatycznym wydłużeniem okresu obowiązywania podpisów kwalifikowanych i certyfikatów kwalifikowanych dla poszczególnych Subskrybentów o kolejne 36 miesięcy następujące bezpośrednio po wygaśnięciu posiadanych przez Zamawiającego certyfikatów i podpisów.
		4. nadanie uprawnień Operatora PPT dla nie więcej niż 15 osób wskazanych przez Zamawiającego, wraz z przeprowadzeniem instruktarzu obsługi PTT;
		5. dostarczenie kwalifikowanych elektronicznych znaczników czasu w liczbie 5 000 miesięcznie dla każdego Certyfikatu kwalifikowanego przez cały okres ważności Certyfikatu kwalifikowanego.
	3. Wymagania dla podpisów elektronicznych

2.3.2.1. opatrzenie każdego podpisu znacznikiem czasu z wykorzystaniem oprogramowania dostarczonego przez Wykonawce.

2.3.2.2 podpisywanie wielu dokumentów jednocześnie w oprogramowaniu dostarczonym przez Wykonawcę .

1. **WYMAGANIA DLA UTRZYMANIA PUNKTÓW POTWIERDZANIA TOŻSAMOŚCI**
	1. Opis sytuacji

3.1.1 Zamawiający posiada 5 Punktów Potwierdzania Tożsamości (PPT).

* + 1. PPT rozlokowane są w różnych lokalizacjach na terenie Polski.
		2. W ramach PPT 15 osób jest uprawnionych do wydawania certyfikatów jako Operatorzy PPT.

 Operatorzy korzystają z dostarczonych urządzeń mobilnych (Terminali), umożliwiających im bezpapierowe/całkowicie elektroniczne wykonywanie wszelkich operacji, w tym rejestracji wniosków elektronicznych o wydanie podpisu elektronicznego i zbierania podpisów osób wnioskujących o podpis elektroniczny. Urządzenia zabezpieczone są oprogramowaniem dostarczonym przez Wykonawcę.

* 1. Wymagania:

3.2.1 Zamawiający zastrzega, że obsługa procesu uzyskania certyfikatu kwalifikowanego odbywać się będzie za pośrednictwem Punktu Potwierdzania Tożsamości jako proces bezpapierowy tj. proces wydawania, przedłużania i unieważniania podpisów elektronicznych realizowany jest całkowicie elektronicznie.

3.2.2 Wykonawca udostępni na czas trwania umowy portal dostępny w Internecie przez przeglądarkę www., w którym operatorzy PPT będą mogli wykonywać czynności polegające na:

3.2.2.1 rejestrowaniu Subskrybentów,

3.2.2.2 rejestrowaniu wniosków o wydanie certyfikatów,

3.2.2.3 weryfikowaniu tożsamości przyszłych Subskrybentów,

3.2.2.4 podpisywaniu umów o świadczenie kwalifikowanych usług zaufania,

3.2.2.5 zgłaszaniu wniosków o unieważnienie certyfikatów,

3.2.2.6 raportowaniu stanu wniosków,

3.2.2.7 raportowaniu aktywnych certyfikatów oraz terminów ich ważności.

3.2.3 Weryfikacja tożsamości realizowana będzie:

3.2.3.1 przez Pracowników Zamawiającego, posiadających autoryzacje centrum certyfikującego Wykonawcy oraz którzy ukończyli egzamin, potwierdzający odpowiednie kwalifikacje,

3.2.3.2 z wykorzystaniem urządzeń mobilnych (Terminali), na których użytkownicy składają podpis elektroniczny za pomocą specjalnego rysika,

3.2.3.3 bezpośrednio z udziałem użytkownika podpisu w dowolnym miejscu na terenie Polski oraz/lub zdalnie za pomocą środków komunikacji na odległość.

3.2.4 Wykonawca zapewni:

3.2.4.1 dostęp do systemu do wydawania, unieważniania oraz zarządzania podpisami elektronicznymi; narzędzie dostępne jako usługa SAAS przez przeglądarkę internetową, niewymagające instalowania dodatkowego oprogramowania,

3.2.4.2 urządzenia mobilne (Terminale) w ilości 6 szt., umożliwiające składanie elektronicznych wniosków o wydanie podpisu elektronicznego oraz weryfikację tożsamości - w dowolnym miejscu na terenie Polski,

3.2.4.3 wszystkie niezbędne uprawnienia i upoważnienia dla pracowników Zamawiającego, umożliwiające im wykonywanie obowiązków Operatorów Punków Potwierdzania Tożsamości, wynikające z podpisanej umowy oraz Polityki Certyfikacji Wykonawcy,

3.2.4.4 system do zarządzania Punktami Potwierdzenia Tożsamości, udostępniony poprzez przeglądarkę www. i niewymagający instalowania dodatkowego oprogramowania,

3.2.4.5 dedykowane wsparcie w procesie uruchamiania i funkcjonowania Punktu Potwierdzania Tożsamości.

3.2.5 Zamawiający zastrzega sobie prawo do wezwania Wykonawcy do prezentacji oferowanego produktu w zakresie niżej wymienionych funkcjonalności:

3.2.5.1 rejestracji wniosku o wydanie certyfikatu za pomocą panelu do usługi dostępu do systemu zarządzania punktów potwierdzania tożsamości,

3.2.5.2 autoryzacji dwuskładnikowej podczas podpisywania dokumentu,

3.2.5.3 podpisywania dokumentu na urządzeniu mobilnym w dowolnej aplikacji do podpisu,

3.2.5.4 rejestrowania zaakceptowanych wniosków o wydanie certyfikatu.

W tym celu Zamawiający zaprosi Wykonawcę i wskaże Wykonawcy przed wyborem najkorzystniejszej oferty termin prezentacji nie krótszy niż 3 dni w siedzibie Zamawiającego lub on-line.

1. **URZĄDZENIA MOBILNE (TERMINALE)**
	1. Wykonawca dostarczy urządzenia mobilne (Terminale), umożliwiające wnioskowanie o wydanie podpisu elektronicznego oraz weryfikacje tożsamości Samsung Tab Active 4 lub równoważne o minimalnych parametrach:

4.1.1 Ekran min. 8”

4.1.2 RAM: 6GB

4.1.3 Pamięć: 128GB

4.1.4 Bluetooth: 5.0

4.1.5 Komunikacja: LTE, Wifi Direct, Wifi 802.11 a/b/g/n/ac, 5G

4.1.6 Gniazda: USB 3.0

4.1.7 W zestawie: rysik S Pen oraz wzmocniona gumowa obudowa

4.1.8 Urządzenia będą objęte gwarancją na warunkach opisanych w Warunkach gwarancji dla urządzeń mobilnych (pkt 5 poniżej).

1. **WARUNKI GWARACJI URZĄDZEŃ MOBILNYCH (TERMINALI)**

5.1 Wykonawca udziela gwarancji jakości na cały okres obowiązywania umowy, na dostarczone urządzenia mobilne.

1. **WYMAGANIA DLA USŁUGI KWALIFIKOWANEGO PODPISU ELEKTRONICZNEGO**

6.1 Ogólne

6.1.1 Format podpisu SHA-2.

6.1.2 Certyfikat kwalifikowany jest powiązany z parą kluczy kryptograficznych o długości min. 3072 bitów.

6.1.3 Certyfikaty powinny być wydawane w powiązaniu z fizyczną kartą kryptograficzną (QSCD - podpis kartowy) lub w przypadku podpisu zdalnego - bez wymaganego czytnika i fizycznej karty kryptograficznej (QSCD zdalne - podpis zdalny).

6.1.4 w przypadku podpisu zdalnego złożenie podpisu wymaga uwierzytelnienia dwuskładnikowego (2FA) oraz podaniem PIN do certyfikatu celem złożenia podpisu pod dokumentem elektronicznym , oraz musi istnieć możliwość złożenia podpisu pod dokumentem w formacie PDF na dowolnym urządzeniu i w dowolnej aplikacji przy czym w przypadku podpisywania dokumentu PDF na urządzeniu mobilnym w aplikacji mobilnej maksymalny rozmiar pliku: co najmniej 10 MB

6.1.5 Okres ważności certyfikatów – 36 miesięcy od daty aktywacji.

6.1.6 Liczba operacji dla każdego certyfikatu – bez limitu.

6.1.7 Kwalifikowany znacznik czasu – 5 000.

6.1.8 Zamawiający ma prawo składać wnioski na poszczególne certyfikaty podpisu elektronicznego przez cały okres trwania umowy.

6.1.9 Wykonawca będzie dostarczał certyfikaty podpisu elektronicznego na podstawie wniosków, składanych drogą elektroniczną w systemie do zarządzania Punktami Potwierdzania Tożsamości przez osoby odpowiedzialne za realizację umowy.

6.1.10 W przypadku odnowienia certyfikatu, Wykonawca umożliwi Subskrybentowi przeprowadzenie samodzielnie całej operacji odnowienia certyfikatu w okresie ważności posiadanego certyfikatu.

6.1.11 Potwierdzenie tożsamości w siedzibie Zamawiającego z wykorzystaniem Punktów Potwierdzania Tożsamości Zamawiającego w formie osobistej

6.1.12 Wymagane znakowanie czasem każdej operacji.

6.1.13 Proces uzyskania certyfikatu kwalifikowanego dostępny w języku polskim oraz angielskim.

6.1.14 Certyfikat musi być wydany przez wystawcę umożliwiającego weryfikację statusu certyfikatu za pomocą list CRL.

6.1.15 Certyfikaty powinny spełniać wymagania określone w przepisach:

6.1.15.1 Certyfikat kwalifikowany w rozumieniu Ustawy z dnia 5 września 2016 roku o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016 poz. 1579, z dnia 05.09.2016), zgodny z wymaganiami określonymi w w/w ustawie oraz rozporządzeniach do w/w ustawy, wydany przez wystawcę wpisanego do „Rejestru podmiotów kwalifikowanych świadczących usługi certyfikacyjne” publikowanego na stronach [www.nccert.pl](http://www.nccert.pl).

6.1.15.2 Certyfikat zgodny z Rozporządzeniem Parlamentu Europejskiego i Rady UE nr 910/2014 z dnia23 lipca 2014 r. „eIDAS” w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.U.UE.910/2014).

6.1.16 Zamawiający wymaga, aby Wykonawca posiadał:

6.1.16.1 Certyfikat ISO 9001 w zakresie usług certyfikacyjnych związanych z podpisem elektronicznym lub równoważny,

6.1.16.2 Certyfikat ISO IEC 27001 w zakresie usług certyfikacyjnych związanych z podpisem elektronicznym lub równoważny,

6.1.16.3 Certyfikat ISO 22301 w zakresie przetwarzania danych osobowych, bezpieczeństwa systemów informatycznych lub równoważny.

6.1.17 Obsługiwany format podpisu przez aplikację podpisującą:

6.1.17.1 XadES, XAdES-T- zgodnie ze specyfikacją ETSI TS 101 903,

6.1.17.2 PadES, PAdES-T- zgodnie ze specyfikacją ETSI TS102 778,

6.1.17.3 CadES.

6.1.18 Obsługiwany typ podpisu:

6.1.18.1 Wewnętrzny otoczony i otaczający - zapis podpisu elektronicznego w tym samy pliku, co podpisywany dokument,

6.1.18.2 Zewnętrzny - zapis podpisu elektronicznego w osobnym pliku,

6.1.18.3 Kontrasygnata i równoległe

6.1.19 Dostawca zobowiązany jest dostarczyć sterowniki do czytników oraz oprogramowanie, umożliwiające złożenie podpisu elektronicznego pod dokumentem elektronicznym oraz umożliwić weryfikację podpisanych dokumentów (wersje językowe PL i EN.):

6.1.19.1 Dostawa w formie elektronicznej.

6.1.19.2 Oprogramowanie i sterowniki muszą być kompatybilne i działać poprawnie na urządzeniach z systemami operacyjnymi Windows 10/11 lub nowszy 64-bit oraz OSX – Catalina, Big Sur, Monterey, Ventura lub nowszy, Android – od v.8.0 i/lub nowszy, dostosowanie do Chromebook, iOS – od v15.0 lub nowszej.

6.1.19.3 Oprogramowanie do zarządzania wirtualną kartą musi zawierać m. in. następujące funkcje: zarządzanie certyfikatami, zarządzanie kartami, rejestracja nowej karty, inicjalizacja kodu PIN i PUK do kart

6.1.19.4 Oprogramowanie do zarządzania kartą fizyczną musi zawierać m.in. następujące funkcje: obsługę profili certyfikatów, znajdujących się na karcie kryptograficznej w formie fizycznej, automatyczne wykrywanie zainstalowanych w systemie czytników kart PCSC, zarządzanie kodami PIN (zmiana lub nadanie kodu PIN), możliwość usuwania certyfikatu z karty, możliwość zarejestrowania umieszczonego na karcie certyfikatu w systemie użytkownika.

6.1.20 Wymagania techniczne do oprogramowania:

6.1.20.1 dostęp do Internetu,

6.1.20.2 system operacyjny: **Windows** 10, Windows 11, **Linux**:Udostępniane paczki oprogramowania są przygotowywane dla systemu Linux, w środowiskach graficznych: Cinnamon, MATE oraz KDE Plasma, **Mac OS X**: od Catalina, Big Sur, Monterey, Ventura

6.1.20.3 komputer klasy PC/laptop: procesor: Pentium 1 GHz (lub zgodny), o pamięci RAM min. 4GB, o min. 200MB wolnej przestrzeni dyskowej przed instalacją aplikacji, rozdzielczość ekranu: 1024x768 lub większa.

6.1.21 Podpisy elektroniczne muszą działać co najmniej w aplikacjach/usługach:

6.1.21.1 Płatnik - http://pue.zus.pl/platnik - podpisanie dokumentów.

6.1.21.2 Platforma ePUAP - http://epuap.gov.pl/ - m.in. podpisywanie korespondenci do wysyłki.

6.1.21.3 Adobe Acrobat Reader - m.in. podpis PAdES z osadzeniem potwierdzenia w treści dokumentu.

6.1.21.4 EPU - Elektroniczne postępowanie upominawcze - https://www.e-sad.gov.pl/ - podpisanie pozwu.

6.1.21.5 Klient JPK - http://www.mf.gov.pl/krajowa-administracja-skarbowa/dzialalnosc/jednolity-plik- kontrolny - podpisanie pliku JPK do wysyłki.

6.1.21.6 TETA ERP - http://www.unit4.com/pl/produkty/erp/teta-erp - m.in. podpisywanie deklaracji podatkowych, dokumentów zakupowych i dokumentów kadrowych.

6.1.21.7 SIGMA - podpisywanie decyzji administracyjnych.

6.1.21.8 SIGMA Mobile - aplikacja na urządzenia mobilne - podpisywanie decyzji administracyjnych.

6.1.21.9 EZD - Elektroniczne Zarządzanie Dokumentacją, wytworzone przez Podlaski Urząd Wojewódzki w Białymstoku.

6.1.21.10 Uwierzytelnianie transakcji bankowych.

6.1.21.11 Aplikacji mobilnej na urządzeniach mobilnych z systemem Android i IOS - podpisywanie dokumentów.

6.1.21.12 Podpisywanie plików, których rodzaje są wymienione w załączniku nr 2 do Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2016 poz. 113).

6.1.21.13 ZSI - podpisywanie protokołów.