

## SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Zamówienie obejmuje sukcesywną dostawę:

1) odnowień certyfikatów kwalifikowanych do podpisu elektronicznego ze standardową kartą kryptograficzną oraz programem do obsługi karty z dwuletnim okresem ważności w maksymalnej liczbie: **130 szt.**

2) certyfikatów kwalifikowanych do podpisu elektronicznego ze standardową kartą kryptograficzną, czytnikiem karty, program do obsługi karty z dwuletnim okresem ważności w maksymalnej liczbie: **15 szt.**

3) zamówienie obejmuje wydanie certyfikatów w siedzibie Zamawiającego (tj. Okręgowy Inspektorat Pracy w Rzeszowie, ul. Gen. St. Maczka 4, 35-234 Rzeszów) oraz oddziałach terenowych (Oddział w Krośnie, ul. Bieszczadzka 1, 38-400 Krosno; Oddział w Przemyślu, ul. Puszkina 14, 37-700 Przemyśl; Oddział w Tarnobrzegu, Pl. B. Głowackiego 52, 39-400 Tarnobrzeg), a także, jeśli zajdzie taka potrzeba, przeszkolenie z obsługi zamawianych zestawów w terminach ustalonych przez Zamawiającego z Wykonawcą.

Szczegółowe parametry elementów zamawianych zestawów określa poniższa tabela.

Element:	Opis:
<i>Certyfikat:</i>	Certyfikat kwalifikowany musi być ważny przez 2 lata.
	Certyfikat kwalifikowany musi być przechowywany w pamięci karty kryptograficznej.
	Dostawca usług certyfikacyjnych musi być kwalifikowanym podmiotem świadczącym usługi certyfikacyjne wpisanym do stosownego rejestru określonego w Rozporządzeniu Parlamentu Europejskiego i Rady UE nr 910/2014 z dnia 23 lipca 2014r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.
<i>Czytnik kart kryptograficznych:</i>	Zgodność ze standardem PC.
	Czytnik oparty na standardzie USB (tzw. token USB)
	Obsługa kart procesorowych zgodnych z normami ISO 7816-1, ISO 7816-2, ISO 7816-3, ISO 7816-4.
	Obsługa kart identyfikacyjnych formatu ID-1 zgodnych z normą ISO/IEC 7810.
	Obsługa protokołów T=0 i T=1.
	Wytrzymałość, co najmniej 100 000 włożeń kart.
	Obsługa w systemach operacyjnych: MS Windows 7/8/10, opcjonalnie Linux.
	Zamawiający wymaga dostarczenia tokenów USB pełniących funkcje czytnika kart kryptograficznych, z zastrzeżeniem, iż muszą spełniać wymogi określone w niniejszym dokumencie.
<i>Karta kryptograficzna:</i>	Karta kryptograficzna wraz z programowaniem do składania bezpiecznego podpisu elektronicznego musi być zgodna z wymogami Rozporządzenia Parlamentu Europejskiego i Rady UE nr 910/2014 z dnia 23 lipca 2014r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.
	Karta kryptograficzna musi być zgodna z normami ISO 7816-1, ISO 7816-2, ISO 7816-3, ISO 7816-4.
	Karta kryptograficzna musi posiadać pamięć nie mniejszą niż 64 kilobajty.
	Karta kryptograficzna musi umożliwiać przechowywanie w swojej pamięci jednej pary kluczy prywatnych do składania bezpiecznego podpisu elektronicznego zgodnego z ustawą o podpisie elektronicznym wraz z certyfikatem kwalifikowanym oraz minimum dwóch par kluczy kryptograficznych dla certyfikatów niekwalifikowanych wraz z certyfikatami, chronionych oddzielnymi kodami PIN dla każdej pary kluczy.
	Karta kryptograficzna musi zapewniać wsparcie dla standardów przemysłowych (PKCS#11, #15, MS CAPI, PC/SC).
	Karta kryptograficzna musi umożliwiać przechowywanie i wykorzystanie kluczy kryptograficznych RSA o długości co najmniej 2048 bitów.
	Wykonawca dostarcza kartę kryptograficzną wraz z oprogramowaniem zarządzającym certyfikatami kwalifikowanym i niekwalifikowanym zapisanymi na karcie kryptograficznej. Dostarczone oprogramowanie musi zapewnić obsługę kart kryptograficznych w systemach operacyjnych MS Windows 7/8/10, opcjonalnie Linux.

	W przypadku dostarczenia tokenów USB pełniących funkcje czytnika kart kryptograficznych Wykonawca musi zapewnić karty kryptograficzne kompatybilne z wyżej wymienionym rozwiązaniem z zastrzeżeniem, iż muszą spełniać wymogi określone w niniejszym dokumencie.
<i>Oprogramowanie:</i>	<p>Wykonawca dostarcza oprogramowanie, które musi umożliwiać składanie bezpiecznego podpisu elektronicznego zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady UE nr 910/2014 z dnia 23 lipca 2014r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.</p> <p><b>Aplikacja musi umożliwiać:</b></p> <p>Masowe i szybkie składanie oraz weryfikacja podpisów, poprzez:</p> <ul style="list-style-type: none"> <li>- wskazywanie wielu plików do strumieniowego podpisania lub weryfikacji,</li> <li>- określenie limitu czasu lub limitu ilości operacji kryptograficznych, do osiągnięcia których możliwe będzie wykorzystywanie komponentu technicznego po jednokrotnym podaniu kodu PIN;</li> <li>- składanie podpisu elektronicznego w jednym z formatów dopuszczonych przez rozporządzenie eIDAS:</li> </ul> <p>* CAdES (PKCS#7) - aplikacja obsługuje warianty: CAdES-BES, CAdES-T, oraz umożliwia składanie podpisu wielokrotnego.</p> <p>* XAdES - aplikacja obsługuje warianty: XAdES-BES, XAdES-T, XAdES-C, XAdES-A oraz umożliwia składanie podpisu wielokrotnego, kontrasygnaty, czy podpisu otoczanego.</p> <p>* PAdES - aplikacja obsługuje warianty: PAdES-BES, PAdES-T, PAdES-LTV.</p> <p>* ASiC-S - aplikacja obsługuje warianty: ASiC-S-CAdES-BES, ASiC-S-XAdES-BES, ASiC-S-CAdES-T, ASiC-S-XAdES-T.</p>

2. Cena ofertowa za wykonanie przedmiotu zamówienia obejmuje wszelkie koszty związane z obsługą formalnoprawną i logistyczną związaną z procesem wydawania i unieważniania certyfikatów.
3. Zamawiający wymaga dostarczenia działających zestawów w ciągu **3 dni roboczych** od dnia złożenia kompletnego wniosku zawierającego niezbędne dane osobowe.
4. Zamawiający nie dopuszcza w ramach realizacji zamówienia dokonywania przedpłat oraz zawierania umów indywidualnych z każdym posiadaczem - użytkownikiem zestawu.
5. Zamawiający dopuszcza możliwość korzystania ze wzoru umowy obowiązującego u Wykonawcy, przy czym wymaga zawarcia w umowie Istotnych dla stron postanowień, które zostaną wprowadzone do treści zawieranej umowy stanowiących Załącznik nr 3 do Zapytania ofertowego z dn. 23.01.2023 r. W przypadku rozbieżności pomiędzy treścią Istotnych dla stron postanowień, które zostaną wprowadzone do treści zawieranej Umowy, a regulaminem świadczenia usług Wykonawcy stosuje się Istotne dla stron postanowienia, które zostaną wprowadzone do treści zawieranej Umowy.