

Opis Przedmiotu Zamówienia (OPZ) – Podpis kwalifikowany

1. Przedmiot zamówienia:

1.1 Przedmiotem zamówienia jest dostawa 1518 sztuk nowych zestawów do składania kwalifikowanego podpisu elektronicznego w formie voucherów ważnych przez okres 60 miesięcy od daty dostarczenia do siedziby Zamawiającego, certyfikowanych zgodnie z rozporządzeniem eIDAS (nr 910/2014) rozporządzenie Parlamentu Europejskiego i Rady (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). Okres ważności kwalifikowanego podpisu elektronicznego określony jest w pkt.2.1

Dodatkowo Wykonawca dostarczy 10 szt. tokenów bez karty, które będą stanowić rezerwę na okres naprawy gwarancyjnej.

1.2 Utworzenie Punktu Obsługi Klienta (Rejestracji):

Wykonawca umożliwi Zamawiającemu pełnienie roli Punktu Rejestracji dla potrzeb wydawania kwalifikowanych podpisów elektronicznych będących przedmiotem zamówienia zwanego dalej POK.

Proces weryfikacji tożsamości oraz przygotowania wniosków certyfikacyjnych będzie realizowany przez wskazanych pracowników Zamawiającego (Operatorów POK).

1.2.1. Obowiązki Wykonawcy:

Przeszkolenie pracowników: Wykonawca przeprowadzi szkolenie dla 9 pracowników Zamawiającego w zakresie procedur weryfikacji tożsamości, obsługi systemu informatycznego Wykonawcy oraz zasad bezpieczeństwa.

Upoważnienia: Wykonawca nada przeszkolonym pracownikom Zamawiającego stosowne upoważnienia/uprawnienia Operatora Punktu Rejestracji, zgodnie z Polityką Certyfikacji Wykonawcy.

Dostarczenie narzędzi: Wykonawca dostarczy instrukcje, procedury oraz dostęp do aplikacji webowej lub oprogramowania niezbędnego do rejestracji wniosków i aktywacji tokenu.

Wsparcie merytoryczne: Wykonawca zapewni dedykowaną linię wsparcia (II linia wsparcia) dla Operatorów Zamawiającego w celu rozwiązywania problemów proceduralnych lub technicznych w trakcie trwania umowy.

2. Logistyka dostaw:

Wykonawca dostarczy 1518 kompletnych zestawów (token USB + karta + licencja) do siedziby Zamawiającego w terminie do 30 dni od podpisania umowy, w stanie "czystym" (do samodzielnej inicjalizacji przez Operatorów Zamawiającego).

2.1 Wymagania techniczne zestawów:

Ważność certyfikatu: Każdy certyfikat musi być ważny przez okres 3 lat (36 miesięcy) od daty jego wydania (aktywacji) z możliwością przedłużenia o kolejne 2 lata (24 miesiące)

Nośnik sprzętowy: Karta kryptograficzna wraz z dedykowanym czytnikiem USB (token), współpracującym ze standardami USB 2.0/3.0.

Oprogramowanie: Wykonawca dostarczy licencję na oprogramowanie do obsługi podpisu, kompatybilne z systemami operacyjnymi Windows (min. 10/11), macOS oraz Linux.

Standardy: Podpis musi umożliwiać generowanie formatów PAdES, XAdES oraz CAdES.

3. Realizacja i weryfikacja tożsamości:

Wykonawca musi zapewnić proces weryfikacji tożsamości dla 1518 użytkowników. Weryfikacja odbywać się w siedzibie Zamawiającego (POK).

Certyfikaty muszą być wydane przez kwalifikowanego dostawcę usług zaufania wpisanego na Listę TSL prowadzoną przez Narodowe Centrum Certyfikacji (NCCert).

4. Gwarancja i wsparcie:

Wykonawca zapewni gwarancję na nośniki fizyczne (tokeny) na cały okres ważności certyfikatu (3 lata).

Bezpłatne wsparcie techniczne (helpdesk) dostępne w dni robocze w godzinach pracy Zamawiającego.

5. Format certyfikatu: W wydawanych certyfikatach numer PESEL podlegać będzie zamianie na identyfikator kadrowy pracownika Zamawiającego. Identyfikatory kadrowe dostarczone będą do Wykonawcy w formularzu zgłoszeniowym. Obowiązkiem Wykonawcy jest powiązanie numeru PESEL z identyfikatorem kadrowym.

Ten sam certyfikat kwalifikowany przypisany do użytkownika musi umożliwiać składanie podpisów zarówno w sieci z dostępem do Internetu jak i w sieci wewnętrznej Zamawiającego.

Zaproponowane rozwiązanie musi zapewnić walidację podpisu kwalifikowanego bez dostępu do Internetu,

Wykonawca zobowiązany jest dostarczać listy CRL raz dziennie w celu ich aktualizacji,

Listy CRL wykorzystywane będą jako źródło informacji o statusie certyfikatu w trybie offline,

Zgodność z RODO: Zastosowane rozwiązanie techniczne musi minimalizować zakres przetwarzanych danych widocznych publicznie, zgodnie z zasadą privacy by design.

Weryfikacja tożsamości w punkcie: Mimo szyfrowania w samym certyfikacie, Operatorzy Zamawiającego w Punkcie Rejestracji muszą mieć możliwość wprowadzenia i zweryfikowania numeru PESEL w systemie Wykonawcy na podstawie okazanego dokumentu tożsamości.