

Opis przedmiotu zamówienia cz.2

1. Certyfikat:

Certyfikat kwalifikowany musi być ważny przez co najmniej 2 lata i przechowywany w pamięci karty kryptograficznej.

Wydawane (wystawiane) kwalifikowane certyfikaty podpisu elektronicznego dla Subskrybentów muszą umożliwiać nielimitowane podpisywanie dokumentów w okresie ważności certyfikatu, autoryzacja podpisu będzie następować poprzez podanie kodu PIN nadawanego przez Subskrybenta (z możliwością jego zmiany). Nie będzie wymagany dostęp do internetu w czasie składania podpisu.

Wystawiony dla Subskrybenta kwalifikowany certyfikat podpisu elektronicznego musi oprócz wymaganych informacji dot. Subskrybenta umożliwiać również podanie innych danych Zamawiającego - minimum: nazwy i adresu Zamawiającego, stanowiska/funkcji Subskrybenta. Podanie tych danych Zamawiającego do certyfikatu jest fakultatywne, będzie określone na etapie składania zamówienia na konkretny certyfikat dla Subskrybenta.

Kwalifikowane certyfikaty podpisu elektronicznego oraz kwalifikowane znaczniki czasu muszą być wystawione przez certyfikowanego dostawcę kwalifikowanych usług zaufania, wpisanego do Rejestru Kwalifikowanych Usług Zaufania (<https://www.nccert.pl/uslugi.htm>) na podstawie przepisów Ustawy z dnia 5 września o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz. U. z 2024 r. poz. 422).

2. Karta kryptograficzna:

Karta formatu karty płatniczej (ID-1).

Karta kryptograficzna (posiadająca certyfikat bezpieczeństwa zgodnie z eIDAS) musi umożliwiać przechowywanie i wykorzystanie kluczy kryptograficznych RSA o długości co najmniej 2048 bitów.

Wykonawca dostarcza kartę kryptograficzną wraz z oprogramowaniem zarządzającym certyfikatem kwalifikowanym zapisanym na karcie kryptograficznej.

Dostarczone oprogramowanie musi zapewnić obsługę kart kryptograficznych w systemach operacyjnych MS Windows 10 i 11 (64 bity).

3. Oprogramowanie:

Wykonawca dostarcza płytę z oprogramowaniem i sterownikami przy czym Zamawiający dopuszcza możliwość udostępnienia oprogramowania i sterowników na stronie internetowej Wykonawcy, jako rozwiązanie równoważne dla płyty z oprogramowaniem i sterownikami.

Oprogramowanie, 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.

Dostarczone Zamawiającemu oprogramowanie do składania podpisu elektronicznego, musi obsługiwać dopuszczone przez rozporządzenie eIDAS formaty podpisu, w tym minimum:

- a. CAdES (PKCS#7) –obsługiwane warianty: CAdES-BES, CAdES-T oraz umożliwia składanie podpisu wielokrotnego;
- b. XAdES –obsługiwane warianty: XAdES-BES, XAdES-T, XAdES-C, XAdES-A oraz umożliwia składanie podpisu wielokrotnego, kontrasygnaty czy podpisu otaczanego;
- c. PAdES –obsługiwane warianty: PAdES-BES, PAdES-T, PAdES-LTV;
- d. ASiC-S – obsługiwane warianty: ASiC-S-CAdES-BES, ASiC-S-XAdES-BES, ASiC-S-CAdES-T, ASiC-S-XAdES-T;
- e. posiadać interfejs oprogramowania w j. polskim,
- f. umożliwiać podpisywanie dokumentów w każdym formacie plików, z zachowaniem reguł dla poszczególnych formatów podpisu elektronicznego.
- g. musi być kompatybilne minimum z systemem operacyjnym Windows 10 i 11 (64 bity),
- h. umożliwiać minimum: podpisywanie dokumentów, dodawanie kolejnych podpisów, kontrasygnata, dodawanie kwalifikowanego znacznika czasu, podpisywanie dokumentów XML wraz z załącznikami kwalifikowanym podpisem elektronicznym;
- i. weryfikować złożony podpis elektroniczny na dokumentach pod kątem jego ważności i poprawności.