PZ-NAI-A.213.2.2022

Załącznik 1B do zapytania ofertowego

Opis przedmiotu zamówienia cz.2

1. Certyfikat:
   Certyfikat kwalifikowany musi być ważny przez co najmniej 2 lata i 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.
2. Karta kryptograficzna:
   Karta formatu karty płatniczej (ID-1).
   Karta kryptograficzna 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 (32 i 64 bity), opcjonalnie Linux.
3. Czytnik kart kryptograficznych (w przypadku odnowienia certyfikatów posiadanych przez Zamawiającego Wykonawca nie ma obowiązku dostarczenia nowego czytnika, jeżeli posiadane przez Zamawiającego czytniki model: OMNIKEY 3021 będą kompatybilne z nowymi kartami):
   Czytnik oparty na standardzie USB
   Obsługa dostarczonych kart kryptograficznych.
   Obsługa w systemach operacyjnych: MS Windows 10 (32 i 64 bity), opcjonalnie Linux. Sterownik zgodny ze standardem Plug&Play, podpisany przez Microsoft (dla systemów Windows).
4. 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.
   Aplikacja musi umożliwiać:
   Masowe i szybkie składanie oraz weryfikację podpisów, poprzez:
   - wskazywanie wielu plików do strumieniowego podpisania lub weryfikacji,
   - określenie limitu czasu lub limitu ilości operacji kryptograficznych, do osiągnięcia których możliwe będzie wykorzystywanie komponentu technicznego po jednokrotnym podaniu kodu PIN;

- składanie podpisu elektronicznego w jednym z formatów dopuszczonych przez rozporządzenie eIDAS:
* CAdES (PKCS#7) - aplikacja obsługuje warianty: CAdES-BES, CAdES-T, oraz umożliwia składanie podpisu wielokrotnego.
* XAdES - aplikacja obsługuje warianty: XAdES-BES, XAdES-T, XAdES-C, XAdES-A oraz umożliwia składanie podpisu wielokrotnego, kontrasygnaty, czy podpisu otaczanego.
* PAdES - aplikacja obsługuje warianty: PAdES-BES, PAdES-T, PAdES-LTV.
* ASiC-S - aplikacja obsługuje warianty: ASiC-S-CAdES-BES, ASiC-S-XAdES-BES, ASiCS-CAdES-T, ASiC-S-XAdES-T.