**Załącznik nr 4 do OPZ**

Opis Systemu Autoryzacji

**System autoryzacji – szt. 1**

**o n/w parametrach:**

1. **Karta mikroprocesorowa (chipowa).**
   1. format karty ID-1 (standardowy format kart płatniczych),
   2. wykonana z materiału PVC,
   3. stykowy interfejs karty,
   4. brak interfejsu bezstykowego,
   5. obszar pamięci nieulotnej na klucze prywatne, certyfikaty i inne obiekty nie mniejszy niż 64 kB,
   6. oprócz obszaru z certyfikatem kwalifikowanym musi posiadać co najmniej dwa dodatkowe obszary dostępne dla użytkownika, w których możliwe jest umieszczenie własnych kluczy i certyfikatów,
   7. użycie konkretnego PINu warunkuje użycie konkretnego certyfikatu i klucza prywatnego - nie dopuszcza się możliwości przechowywania przez zainicjalizowaną kartę tylko jednego zestawu (PIN, PUK, certyfikat, klucz prywatny), karta w zależności od PINu może użyć innego certyfikatu (np. kwalifikowanego lub nie) tej samej osoby.
   8. długość kodu PIN nie może być mniejsza niż 6 cyfr,
   9. długość kodu PUK nie może być mniejsza niż 8 cyfr,
   10. użycie klucza prywatnego tylko po podaniu kodu PIN użytkownika,
   11. po trzykrotnym błędnym podaniu kodu PIN karta zostaje zablokowana,
   12. odblokowanie jest możliwe jedynie po podaniu kodu PUK,
   13. po trzykrotnym błędnym podaniu kodu PUK karta zostaje trwale zablokowana,
   14. karta musi posiadać ważny certyfikat potwierdzający spełnienie wymagań dla kwalifikowanego urządzenia do składania podpisu elektronicznego (zgodnie z Wymaganiami dla kwalifikowanych urządzeń do składania podpisu elektronicznego określonych w załączniku II do Rozporządzenia 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 uchylającym dyrektywę 1999/93/WE).
   15. spełnia zgodność z normą ISO 7816 (części 1, 2, 3, 4, 5, 6, 7, 8, 9 oraz aneksy A, B, C, D, E, F) - szczególnie części:
       1. Basic Organizations,
       2. Basic Interindustry Commands,
       3. Transmission Oriented Interindustry Commands,
       4. Transportation of APDU messages by T=0,
       5. Transportation of APDU messages by T=1,
       6. standardy przemysłowe komend i protokołów komunikacyjnych T=0 i T=1 (z wyłączeniem wykluczających się, dopuszczonych przez powyższą normę opcji,
   16. obsługa kluczy kryptograficznych RSA 2048 bitów,
   17. obsługa funkcji skrótu SHA-256,
   18. obsługa algorytmów DES, 3DES,
   19. oprogramowanie komunikacyjne MS CSP i PKCS#11,
   20. system operacyjny umożliwiający wieloaplikacyjność,
   21. certyfikat bezpieczeństwa układu mikroprocesorowego na poziomie ITSEC E3,
   22. karta musi zostać spersonalizowana dla użytkownika w taki sposób, aby na awersie karty widoczne było jego imię i nazwisko naniesione na trwale,
   23. współpraca z systemem operacyjnym Microsoft Windows XP/7/8/8.1/10 w wersji 32 i 64 bitowej oraz Linux,
   24. Zamawiający nie ponosi odpowiedzialności za uszkodzenia karty wynikłe nie z jego winy,
   25. w ramach gwarancji Zamawiający wymaga, aby w przypadku awarii/problemów, Wykonawca zapewnił wymianę karty z certyfikatem trzech dni roboczych od złożenia reklamacji,
2. **Czytnik kart mikroprocesorowych (chipowych).**
   1. fabrycznie nowy, wyprodukowany nie wcześniej niż 12 miesięcy przed data dostawy,
   2. zewnętrzny,
   3. dołączany do komputera przez złącze USB,
   4. wtyk USB typ A,
   5. zasilanie przez złącze USB,
   6. komunikacja z komputerem poprzez dwukierunkowy interfejs USB 2.0,
   7. zgodność z USB1.1 i 3.0)
   8. długość kabla minimum 1,2 m,
   9. interfejs karty stykowy,
   10. trwałość styków nie mniej niż 100 000 cykli,
   11. sygnalizacja optyczna gotowości czytnika i pracy z kartą,
   12. format karty ID-1 (standardowy format kart płatniczych),
   13. zapis i odczyt kart wykonanych zgodnie ze normą ISO 7816 (części 1, 2, 3, 4 aneksy A, B, C) oraz klasy A, B i C (5V; 3V; 1,8V)
   14. standardy PC/SC, CT-API, „Plug and Play” Microsoft,
   15. obsługiwane protokoły: T=0, T=1, I2C, 2WBP, 3WBP,
   16. czytnik kart musi umożliwiać obsługę uwierzytelniania kartą przy pomocy PIN,
   17. czytnik kart musi działać z systemami operacyjnymi Microsoft Windows 7 i nowsze, Windows Serwer 2012 i nowsze oraz Linux i Mac OS X,
3. **Oprogramowanie.**
   1. graficzny interfejs użytkownika w języku polskim,
   2. obsługa czytnika i karty mikroprocesorowej,
   3. możliwość weryfikacji i podpisywania dokumentów (w tym podpisu wielokrotnego) z wykorzystaniem kwalifikowanych certyfikatów,
   4. składanie podpisu w formatach dopuszczonych przez rozporządzanie eIDAS: CAdES, XAdDES, PAdDES,
   5. musi umożliwiać korzystanie z usługi oznaczania czasem,
   6. musi umożliwiać składanie podpisu w formacie umożliwiającym zachowanie długoterminowej ważności dowodowej podpisu elektronicznego i zawierającym następujące informacje:
   7. podpisy wielokrotne,
   8. certyfikaty osób podpisujących jako atrybuty podpisane,
   9. znaczniki czasu,
   10. ścieżki certyfikacji,
   11. listy unieważnionych certyfikatów,
   12. identyfikatory polityk podpisu,
   13. format podpisu elektronicznego musi zapewnić długoterminową archiwizację dokumentów opatrzonych podpisem bezpiecznym,
   14. Dostarczane oprogramowanie musi posiadać deklarację producenta o zgodności z polskim prawem,
   15. musi zapewniać odczyt i weryfikację elektronicznych podpisów kwalifikowanych wydanych przez centra certyfikacji autoryzowane w wyżej wymienionym zakresie na terenie RP,
   16. musi zawierać zestaw bibliotek programistycznych, które pozwalają na implementację funkcjonalności związanych z podpisem elektronicznym w oprogramowaniu i w systemach nie związanych z PKI. Pozwalają na implementację obsługi: podpisu elektronicznego, szyfrowania danych, weryfikacji certyfikatu w trybie on-line, na znakowanie wiarygodnym czasem,
   17. do oprogramowania musi być dołączony podręcznik użytkownika w języku polskim (dopuszcza się wersję elektroniczną instrukcji - format PDF lub DOC),
   18. oprogramowanie musi umożliwiać wybór czytnika (Zamawiający posiada stacje robocze z czytnikami kart przeznaczonymi do obsługi własnego systemu zarządzania tożsamością) i certyfikatu,
   19. licencja musi uprawniać do wykorzystywania oprogramowania na każdym stanowisku pracy, na którym wykorzystywana jest karta zawierająca certyfikat,
   20. Zamawiający wymaga potwierdzenia przez Wykonawcę, że oprogramowanie ma funkcje podpisu, która są wymagane ustawowo,
   21. oprogramowania musi być aktualizowane przez czas trwania umowy, aby pozostawało w zgodzie z prawem,
   22. Kompatybilność ze sprzętem komputerowym o minimalnych parametrach:
       1. Procesor Pentium 800 MHz
       2. Pamięć 512 MB
       3. Miejsce na dysku 100 MB
       4. Porty USB
       5. system operacyjny Microsoft Windows XP/7/8/8.1/10 w wersji 32 i 64 bitowej oraz Linux,
       6. Przeglądarka Internetowa Mozilla Firefox, Google Chrome, Internet Explorer, Opera,
   23. obsługa kart kryptograficznych wydanych przez wszystkie kwalifikowane centra certyfikacji działające na polskim rynku,
   24. oprogramowanie musi posiadać możliwość aktualizacji na stacjach roboczych,
   25. automatyczne informowanie o nowej wersji oprogramowania do pobrania,
4. Obsługa list TSL umożliwiająca weryfikację podpisów z krajów UE,
5. **Certyfikat kwalifikowany.**
   1. certyfikat kwalifikowany zgodny z ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016 poz. 1579),
   2. wydany przez wystawcę wpisanego do „Rejestru podmiotów kwalifikowanych świadczących usługi certyfikacyjne” publikowanego na stronach www.nccert.pl,
   3. ważność certyfikatu 2 lata z możliwością odnowienia na kolejny rok lub 2 lata,
   4. musi być powiązany z parą kluczy kryptograficznych o długości 2048 bitów, generowanych przy użyciu algorytmu RSA,
   5. musi zawierać skrót wykonany za pomocą algorytmu SHA-2,
   6. certyfikat musi umożliwiać zapisanie na żądanie Zamawiającego dodatkowych danych, które nie będą burzyły struktury certyfikatu,
   7. certyfikat powinien być wydany przez wystawcę umożliwiającego weryfikację statusu certyfikatu za pomocą listy CRL,
   8. lista CRL nie może być generowana rzadziej niż raz dziennie,
   9. wystawienie certyfikatu musi być realizowane na podstawie wniosku bez konieczności wizyty użytkownika w punkcie rejestracji,
   10. certyfikat zostanie dostarczony na karcie elektronicznej opisana w punkcie 1.