**Specyfikacja kart mikroprocesorowych kompatybilnych z systemem użytkowanym
u Zamawiającego:**

1. Karty zgodne z normą ISO-7816 część 1,2,3,4.
2. Obszar pamięci na dane pozwalający na przechowywanie min. 3 kluczy RSA 2048 bity oraz min. 3 certyfikatów o rozmiarze 2kB każdy.
3. Karty realizują podpis algorytmem RSA przy użyciu klucza prywatnego znajdującego się na karcie. Zaimplementowany algorytm RSA jest zgodny ze specyfikacją PKCS#1 w wersji 1.5.
4. Karta obsługuje protokoły T=0, T=1.
5. Wraz z kartą dostarczona jest biblioteka dynamiczna DLL z implementacją interfejsu PKCS#11 w wersji co najmniej 2.0 oraz oprogramowanie zarządzające kartą dla systemów min. Windows7/8/10/11.
6. Karty umożliwiają generowanie kluczy kryptograficznych na karcie.
7. Karty umożliwiają wygenerowanie i przechowywanie, co najmniej trzech par kluczy asymetrycznych RSA o długości co najmniej 2048 bitów (jedna para do uwierzytelniania, druga do podpisu i trzecia do szyfrowania), oraz zapis kluczy prywatnych wygenerowanych poza kartą wraz z certyfikatami.
8. Karta umożliwia elastyczne definiowanie profilu definiującego zasady kontroli dostępu do obiektów chronionych na karcie, w tym co najmniej:
9. możliwość definiowania min. 3 odrębnych kodów typu PIN oraz jednego lub więcej odrębnych kodów typu PUK służących do odblokowania zablokowanych kodów PIN;
10. możliwość definiowania min. i max długości każdego kodu PIN oraz PUK oraz ilości błędnych prób ich podawania, po których następuje zablokowanie dostępu do kluczy prywatnych i obiektów danych chronionych danym kodem;
11. możliwość swobodnego wybierania podczas generowania lub zapisywania danych kodu PIN, który będzie chronił dostępu do tych danych;
12. możliwość zapewnienia, iż końcowy użytkownik karty jest jedyną osobą, która posiada dostęp do kluczy prywatnych wygenerowanych na jego karcie.
13. Wielokrotne usuwanie i zapisywanie ponownie kluczy kryptograficznych i obiektów danych nie powoduje zmniejszania się dostępnej pamięci na te dane poniżej progu pozwalającego na przechowywanie wskazanych w pkt 2 i 7 danych (karta zarządza dynamicznie przydziałem i zwalnianiem pamięci).
14. Karta udostępniana przez oba interfejsy (PKCS#11 i MS CSP/KSP) umożliwia pracę wieloaplikacyjną (jednoczesne używanie karty przez wiele aplikacji). Klucze i obiekty danych zapisywane za pośrednictwem jednego interfejsu są dostępne dla drugiego interfejsu, jeżeli cechy zapisywanych jednym interfejsem kluczy i danych nie wykraczają poza specyfikację drugiego interfejsu i możliwe jest wzajemne mapowanie tych informacji.
15. Karty są bezterminowe (tzn. nie posiadają terminu ważności).
16. Karta wspiera środowiska Windows w wersjach min., Windows7 SP1, Windows 8, Windows 10, Windows 11, Serwer 2008 SP2 i nowszych (obsługa systemów operacyjnych 32/64bit).

Dostarczone wraz z kartami oprogramowanie zarządzające, biblioteki dll, licencje umożliwiają współpracę z posiadanym przez Zamawiającego aplikacjami dla użytkowników końcowych,
z PKI opartym o oprogramowanie Centaur CCK i Centaur PR.

Chip na karcie mikroprocesorowej jest niewyłamywalny, tj. karta nie posiada wokół niego nacięć umożliwiających oddzielenie części elektronicznej od reszty karty.