

Specyfikacja kart mikroprocesorowych.

1. Karty muszą być 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 muszą realizować podpis algorytmem RSA przy użyciu klucza prywatnego znajdującego się na karcie. Zaimplementowany algorytm RSA musi być zgodny ze specyfikacją PKCS#1 w wersji 1.5.
4. Karta musi obsługiwać protokoły T=0 albo T=1.
5. Wraz z kartą musi być dostarczona 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 muszą umożliwiać generowanie kluczy kryptograficznych na karcie.
7. Karty muszą umożliwiać 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:
 - a) Możliwość definiowania min. 3 odrębnych kodów typu PIN oraz jednego lub więcej odrębnych kodów typu PUK służących do odblokowania zablokowanych kodów PIN
 - b) 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.
 - c) Możliwość swobodnego wybierania podczas generowania lub zapisywania danych kodu PIN, który będzie chronił dostęp do tych danych.
 - d) Możliwość zapewnienia, iż końcowy użytkownik karty jest jedyną osobą, która posiada dostęp do kluczy prywatnych wygenerowanych na jego karcie
9. 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).
10. 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.
11. Karty muszą być bezterminowe (tzn. nie posiadają terminu ważności).
12. Karta musi wspierać 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 muszą umożliwiać współpracę z posiadanym przez Policję aplikacjami Zamawiającego dla użytkowników końcowych, z PKI opartym o oprogramowanie Centaur CCK i Centaur PR. Powyższe będzie podlegało procesowi weryfikacji podczas procedury testowej, która to opisana zostanie w Opisie Przedmiotu Zamówienia.

Chip na karcie mikroprocesorowej nie może być wylamywalny, tj karta nie może posiadać wokół niego nacięć umożliwiających oddzielenie części elektronicznej od reszty karty.

Dla kart nie jest wymagana personalizacja typu: elementy graficzne, hologram.