Załącznik nr 1

**Szczegółowy opis przedmiotu zamówienia**

**Wymagania dotyczące kart mikroprocesorowych:**

1. Karty muszą być zgodne z normą ISO-7816 część 1,2,3,4

2. Obszar pamięci na dane (klucze prywatne, certyfikaty i inne obiekty) - 64 KB (min. 32 KB).

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/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. Windows 7, Windows 8,   
Windows 10, Windows 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 dostępu 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 (karta zarządza dynamicznie przydziałem i zwalnianiem pamięci).

10. Karta pozwala na efektywne i elastyczne wykorzystanie pamięci na dane i nie rezerwuje na sztywno obszarów pamięci danych bez ich rzeczywistego wykorzystania

11. 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.

12. Wykonawca dostarczy opis dostępnych parametrów konfigurowalnych w ramach profilu karty.

13. Możliwość zabezpieczonej, ponownej inicjalizacji zablokowanej karty bez możliwości dostępu do zablokowanych sekretów (karta z zablokowanymi kodami PUK może być sformatowana i ponownie użyta, ale obiekty zablokowane ulegają bezpowrotnemu skasowaniu).

14. Karty muszą być bezterminowe (tzn. nie posiadają terminu ważności).

15. 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).

16. Karta musi współpracować z posiadanym przez Policję Centralnym Policyjnym Systemem Autoryzacji funkcjonującym w Policyjnej Sieci Transmisji Danych. Przetestowane i obecnie współpracujące z w/w systemem autoryzacji karty to: CRYPTOTECH MULTI SIGN, OBERTUR ID ONE ENCARD. W przypadku zaoferowania innej karty Wykonawca zobowiązany jest dostarczyć z ofertą opis dostępnych parametrów zawartych w pliku konfigurującym profil inicjowanej karty. W przypadku zaoferowania innej karty Zamawiający przeprowadzi testy funkcjonalne tej karty w celu sprawdzenia czy współpracuje ona z posiadanym przez Policję Centralnym Policyjnym Systemem Autoryzacji.