Załącznik nr 1

**Szczegółowy opis przedmiotu zamówienia**

 **Wymagania dotyczące kart mikroprocesorowych:**

1. Karty muszą być zgodne z normą ISO-7816 część 1,2,3,4,8.
2. 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.
3. Wraz z kartą musi być dostarczona biblioteka dynamiczna DLL oraz oprogramowanie zarządzające dla systemów Windows XP/Vista, Windows7, Windows 8, Windows 10 z implementacją interfejsu PKCS#11 w wersji co najmniej 2.01. Implementacja interfejsu musi być zgodna ze standardem PKCS#11 opublikowanym przez firmę RSA SECURITY.
4. Karty muszą umożliwiać generowanie kluczy na standardowych kartach kryptograficznych, zgodnych z interfejsem PKCS#11 i formatem PKCS#15.
5. Karty muszą umożliwiać wygenerowanie i zapisanie, co najmniej dwóch par kluczy asymetrycznych RSA o długości od 1024 bitów do 2048 bitów (jedna para do uwierzytelniania, druga do podpisu i szyfrowania), oraz zapis kluczy prywatnych wraz z certyfikatami.
6. Karta umożliwia elastyczne definiowanie profilu definiującego zasady kontroli dostępu do obiektów chronionych na karcie, w tym co najmniej:
7. Możliwość definiowania min. 1 kodu PIN oraz związanego z nim 1 kodu PUK (odblokowanie zablokowanego kodu PIN).

b) Możliwość definiowania min. i max długości 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 definiowania ilości operacji dostępu do danych, na którą ważne jest jednorazowe podanie danego kodu PIN (1, kilka operacji, brak limitu).

d) Możliwość swobodnego wybierania podczas generowania lub zapisywania danych kodu PIN, który będzie chronił dostępu do tych danych.

e) Możliwość zapewnienia, iż końcowy użytkownik karty jest jedyną osobą, która posiada dostęp do kluczy prywatnych wygenerowanych na jego karcie .

1. 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).
2. Karta pozwala na efektywne i elastyczne wykorzystanie pamięci na dane i nie rezerwuje na sztywno obszarów pamięci danych bez ich rzeczywistego wykorzystania (np. nie jest dopuszczalne sztywne definiowane ilości pamięci przeznaczonej na klucze, certyfikaty, dowolne dane).
3. Definiowanie profilu pamięci karty, ilości kodów PIN/PUK, ich parametrów (długości, ilości błędnych prób, itd.) jest możliwe wielokrotnie przez Zamawiającego.
4. Karta udostępniana przez oba interfejsy (PKCS#11 i MS CSP) umożliwia pracę wieloaplikacyjną (jednoczesne używanie karty przez wiele aplikacji). Klucze i obiekty danych zapisywane za pośrednictwem jednego interfejsu są dostępne dla drugiego interfejsu.
5. Możliwość zabezpieczonej, ponownej inicjalizacji zablokowanej karty bez możliwości dostępu do zablokowanych sekretów (karta z zablokowanymi kodem/kodami PUK może być sformatowana i ponownie użyta, ale obiekty zablokowane ulegają bezpowrotnemu skasowaniu).
6. Karty muszą być bezterminowe (tzn. nie posiadają terminu ważności).
7. Karta musi wspierać środowiska Windows XP i 2003, 2008, Vista, Windows7, Windows 8, Windows 10 (obsługa systemów operacyjnych 32/64bit).
8. 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.
9. Karty muszą być niezainicjowane.

**Po wyborze najkorzystniejszej oferty (przed podpisaniem umowy) wybrany Wykonawca,
w terminie 2 dni od daty zakończenia postępowania dostarczy na własny koszt Zamawiającemu 1 egz. zamawianego asortymentu (karty mikroprocesorowej) celem przeprowadzenia testu funkcjonalnego weryfikującego poprawność współpracy z posiadanym przez Policję Centralnym Policyjnym Systemem Autoryzacji.**

**Procedura testowa do testów funkcjonalnych karty mikroprocesorowej weryfikujących jej współpracę z posiadanym przez Policję Centralnym Policyjnym Systemem Autoryzacji**

|  |  |  |
| --- | --- | --- |
| **Lp.**  | **Rodzaj testu** | **Wynik testu pozytywny (TAK/NIE)** |
| 1. | Zaprogramowanie karty w Punkcie Rejestracji |  |
| 2. | Autoryzacja w systemie BTUU z wykorzystaniem zaprogramowanej karty |  |
| 3. | Autoryzacja w systemie SWD z wykorzystaniem zaprogramowanej karty |  |
| 4. | Autoryzacja w systemie Win XP Pro 32-bit z wykorzystaniem zaprogramowanej karty i oprogramowania E-GINA ver. 2.0  |  |