

## Opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostawa hybrydowych elektronicznych kart procesorowych z dwoma interfejsami w ilości 1000 szt.

Specyfikacja techniczna:

- 1.1.1. Karta procesorowa musi być kartą hybrydową;
- 1.1.2. Interfejs stykowy musi być zgodny z normami ISO/IEC 7816-2 i ISO/IEC 7816-3 o pojemności pamięci EEPROM co najmniej 67 kilobajtów
- 1.1.3. Interfejs bezstykowy musi być zgodny z normą ISO/IEC 14443 typ A, zgodnym ze standardem przemysłowym MIFARE® dla protokołu klasycznego o pojemności pamięci 1 kilobajt (MIFARE® Standard Card IC MF1 IC S50 Functional Specification).
- 1.1.4. Wymagania dla części elektronicznej – stykowej**
  - 1.1.4.1. Część stykowa karty jest wyposażona w interfejs określony w normach ISO/IEC 7816-2 i ISO/IEC 7816-3.
  - 1.1.4.2. Polecenia i odpowiedzi przesyłane podczas komunikacji Karty z infrastrukturą informatyczną powinny mieć strukturę zgodną z APDU określoną w normie ISO/IEC 7816-4.
  - 1.1.4.3. Polecenia realizowane przez Kartę dla operacji kryptograficznych i zarządzania są zgodne z ISO/IEC 7816-8, ISO/IEC 7816-9 oraz opcjonalnie ISO/IEC 7816-15.
  - 1.1.4.4. Blankiet karty hybrydowej musi spełniać następujące wymagania:
  - 1.1.4.5. Układ elektroniczny o pojemności pamięci EEPROM co najmniej 67 kilobajtów z wbudowanym koprocesorem kryptograficznym.
  - 1.1.4.6. Układ elektroniczny blankietu karty musi posiadać certyfikat Common Criteria Standard na poziomie co najmniej EAL4+.
  - 1.1.4.7. Card Management i API zgodne z Global Platform 2.1.1
  - 1.1.4.8. System operacyjny Java Card Virtual Machine, RTE i API zgodne z JC2.2.1
  - 1.1.4.9. Blankiet karty musi posiadać certyfikat Common Criteria Standard według profilu PPSSCD Protection Profile – Secure Signature Creation Device Type 2 and/or 3, version 1.05, EAL4+ (CWA14169).
  - 1.1.4.10. Zgodny ze standardem funkcjonalności E-Sign K (CWA14890).
  - 1.1.4.11. DAP zgodne z Global Platform 2.1 (PK-Based).
  - 1.1.4.12. Obsługiwane protokoły: T=0, T=1, PPS.
  - 1.1.4.13. Prędkość transmisji czytnik – karta do 230 Kbauds.
  - 1.1.4.14. Dostęp do klucza prywatnego zapisanego na Karcie możliwy jest wyłącznie przez koprocesor kryptograficzny Karty.
  - 1.1.4.15. Wszystkie operacje kryptograficzne dotyczące klucza prywatnego wykonywane na karcie.
  - 1.1.4.16. Użycie klucza prywatnego tylko po podaniu kodu PIN użytkownika.
  - 1.1.4.17. Generowanie kluczy kryptograficznych o długości do 2048 bitów przeznaczonych do użycia przez algorytm RSA, podpisywanie za pomocą algorytmu RSA, obsługa funkcji skrótu SHA-1, SHA-256, obsługa algorytmów DES, 3DES (ECB, CBC), AES.
  - 1.1.4.18. Karta przystosowana do umieszczenia na niej certyfikatu kwalifikowanego wraz z kluczami kryptograficznymi oraz certyfikatu niekwalifikowanego wraz z kluczami kryptograficznymi; certyfikaty mogą zostać umieszczone w późniejszym czasie.
- 1.1.5. Wymagania dla części elektronicznej – bezstykowej**
  - 1.1.5.1. Część bezstykowa jest wyposażona w interfejs zgodny z ISO/IEC 14443 typ A.

- 1.1.5.2. Sposób komunikacji karty jest zgodny ze standardem przemysłowym MIFARE® dla protokołu klasycznego spełniającym wymagania normy ISO/IEC 14443-1, ISO/IEC 14443-2, ISO/IEC 14443-3 oraz ISO/IEC 14443-4 (protokół T=CL), przy zachowaniu pełnej antykolizyjności.
- 1.1.6. Karta musi współpracować z systemem OPTIcamp firmy OPTeam S.A. (OPTeam S.A. ul. Tajęcina 113, 36-002 Jasionka) zaimplementowanym w Uniwersytecie Jana Kochanowskiego w Kielcach.
- 1.1.7.

Warunki gwarancji :

Okres gwarancji: minimum 12 miesięcy.

Nieodpłatna wymiana wadliwych kart na pozbawione wad karty.