

OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa jednorazowa blankietów elektronicznej karty procesorowej:

Elektronicznej Legitymacji Studenta – 2500 sztuk

zgodnie z poniższym Opiszem Przedmiotu Zamówienia.

Zaoferowane blankiety muszą być zgodne z Rozporządzeniem Ministra Nauki i Szkolnictwa Wyższego z dnia 16 kwietnia 2019 r. zmieniające rozporządzenie w sprawie studiów

Zamawiający dla potrzeb personalizacji kart procesorowych wykorzystuje blankiety Thales (Gemalto) 941B Mifare 1k z nadrukiem, które zostały pozytywnie zweryfikowane.

Warunkiem udziału w postępowaniu będzie pozytywna weryfikacja poprawności i zgodności karty z systemem Zamawiającego w siedzibie Zamawiającego w uzgodnionym dniu.

WYMAGANIA TECHNICZNE (warunki równoważności) ODNOŚNIE BLANKIETÓW ELS:

Wymagana jest elektroniczna karta procesorowa, o pojemności pamięci typu **EEPROM wynoszącej co najmniej 110 kilobajtów, karta hybrydowa z dwoma niezależnymi interfejsami:**

1 stykowym:

- zgodność z ISO/IEC 7816-1, 7816-2 i 7816-3 (protokół T=0, T=1);
- polecenia i odpowiedzi przesyłane podczas komunikacji karty z infrastrukturą informatyczną mają strukturę zgodną z APDU określoną w normie ISO/IEC 7816-4;
- polecenia realizowane przez kartę dla operacji kryptograficznych i zarządzania są zgodne z normą ISO/IEC 7816-8, ISO/IEC 7816-9;
- pojemność pamięci typu flash – min. 344 KB

2 bezstykowym:

- zgodność z ISO/IEC 14443-1, 14443-2, ISO/IEC 14443-3
- polecenia i odpowiedzi przesyłane podczas komunikacji karty z infrastrukturą informatyczną mają strukturę zgodną z określoną w normie ISO/IEC 14443-4 oraz umożliwiają realizację poleceń APDU ze zbioru określonego dla interfejsu bezstykowego (protokół T = CL);
- określony w normie ISO/IEC 14443 typ A, zgodny ze standardem przemysłowym **MIFARE® Classic EV1** dla protokołu klasycznego o pojemności pamięci 1 kilobajt (**wymagany moduł MIFARE® Standard Card EV1 MF1 IC S50 MOA8 4B** Functional Specification);

Poddruk wykonany dla **wersji studenckiej ELS** - według wzoru określonego w załączniku nr 1 rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 16 kwietnia 2019 r. zmieniające rozporządzenie w sprawie studiów (Dz. U. 2019 poz. 787) wraz z późniejszymi zmianami.

Białe pole po stronie rewersowej jest położone w stosunku do brzegów karty z dokładnością +/- 0,5 mm.

- 3 Karty wykonane z materiału laminowanego nieulegającemu odkształceniu i/lub rozwarstwieniu o wymiarach i właściwościach fizycznych zgodnych z wymaganiami dla kart identyfikacyjnych formatu ID-1 określonymi w normie ISO/IEC 7810, a jego właściwości i odporność są potwierdzone badaniami przeprowadzonymi zgodnie z wieloczęściową normą ISO/IEC 10373.

PROCESOR STYKOWY

- 1 Wymagana charakterystyka systemu operacyjnego

(niezbędne do poprawnej współpracy z systemem zarządzania wykorzystywanym przez Zamawiającego):

- oparty na maszynie wirtualnej **Java Card w wersji 3.0.4 lub wyższej**, zapewniający wieloaplikacyjność, umożliwiający wprowadzanie różnych typów obiektów (plików, aplikacji, certyfikatów) w bezpiecznym środowisku zarządzania kartą
- zgodny ze standardem **Global Platform Card Specification w wersji 2.2.1 lub wyższej**
- zgodny z **protokołem bezpieczeństwa SCP 01, SCP 02 lub SCP 03**
- posiada **funkcję zarządzania DAP** poprzez Global Platform (dla autoryzacji i weryfikacji)

- 2 Wymagane standardy kryptograficzne obsługiwane przez układ procesorowy:

- **DES, 3DES** (ECB, CBC)
- **AES** (128, 192 oraz 256 bits)
- **RSA** (2048 bits, z opcją rozszerzenia do 4096 bits)
- **ECC** (224 oraz 521 bits)
- funkcja skrótu **SHA-1, SHA-224, SHA-256, SHA-384, SHA-512**

- 3 Wymagane certyfikaty bezpieczeństwa:

- Certyfikat **Common Criteria Standard na poziomie EAL5+**
- Certyfikat **FIPS PUB 140**
- Certyfikat **EMVCo**

- 4 Preinstalowane aplety

(niezbędne do poprawnej współpracy z systemem zarządzania wykorzystywanym przez Zamawiającego):

- zarządzanie kartą (**Card Manager**);
- system plików zgodny z normą ISO/IEC 7816 (**możliwość swobodnego tworzenia plików typu DF i EF**, również po wydaniu karty oraz zabezpieczania zapisu do nich kluczami globalnymi lub lokalnymi)
- **indywidualny aplet** środowiska JavaCard pozwalający na bezpośrednią komunikację z systemem Zamawiającego również poprzez polecenia APDU

PROCESOR BEZSTYKOWY

- 1 Charakterystyka układu

(niezbędna do poprawnej współpracy z systemem zarządzania wykorzystywanym przez Zamawiającego):

- wyposażony w interfejs zbliżeniowy zgodny z normą ISO/IEC 14443 typ A o pojemności pamięci 1 kilobajt, posiadający stały, nadawany na etapie produkcji identyfikator układu (UID) o długości 4B.

- sposób komunikacji karty jest zgodny ze standardem przemysłowym **MIFARE® Classic EV1 na częstotliwości 13,56MHz** dla protokołu klasycznego spełniającego wymagania normy ISO/IEC 14443-1, 14443-2 oraz 14443-3 przy zachowaniu pełnej antykolidyjności.

PARAMETRY OGÓLNE

1 Parametry pracy układu procesorowego

(minimalne, niezbędne do poprawnej współpracy z systemem zarządzania wykorzystywanym przez Zamawiającego):

- Ilość cykli zapis/odczyt – 500 000 cykli
- Szybkość transmisji danych – 446 kbit/s
- Szybkość transmisji typu VHBR dla PICC/PCD 3.2Mbits/s
- Szybkość odpowiedzi układu – poniżej 200ms
- Trwałość danych – 20 lat
- Temperatura pracy – zakres od -25°C do +85°C

2 Charakterystyka układu elektronicznego oraz systemu operacyjnego daje możliwość:

- składania na karcie podpisu elektronicznego w oparciu o biblioteki standardu PKCS#11
- przystosowania karty do umieszczenia na niej certyfikatu wraz z kluczami kryptograficznymi (funkcjonalność PKI); certyfikaty mogą zostać umieszczone w późniejszym czasie; liczba certyfikatów możliwych do umieszczenia na karcie ograniczona jest jedynie pojemnością karty
- stosowania karty jako komponentu technicznego do sprzętowego zabezpieczenia komputera (za pomocą osobnej aplikacji/apletu): wyjęcie karty z czytnika – zablokowanie dostępu do komputera, włożenie karty do czytnika i podanie kodu PIN - odblokowanie dostępu do komputera.

DOKUMENTACJA

W przypadku dostarczenia blankietów innych niż aktualnie używa Zamawiający Wykonawca udostępni Zamawiającemu:

- Specyfikację techniczną karty (**ma być dołączona na etapie postępowania**)
- Dokumentację techniczną preinstalowanych pakietów i apletów (**ma być dołączona wraz z kartami**)
- Dokumentację techniczną oprogramowania dostarczanego z kartą (**ma być dołączona wraz z kartami**)

ZABEZPIECZENIE NA CZAS DOSTAWY

Zamawiający wymaga, aby karty zostały dostarczone z **unikalnymi kluczami transportowymi** dla części bezstykowej (MIFARE®) i stykowej (dostęp do układu procesorowego).

WYMAGANIA DODATKOWE

1. Struktura i architektura układu oraz preinstalowanych apletów **musi być zgodna z aktualnie wykorzystywanym, indywidualnym systemem obsługi kart elektronicznych ELS przez Zamawiającego.**

Oprogramowanie podpisujące legitymacje po stronie Zamawiającego napisane zostało w Java SE 8.

Jest to aplikacja desktopowa z GUI uruchamiana za pośrednictwem formatek zbudowanych w Oracle Forms Builderze, która pobiera dane za pomocą sterownika JDBC z bazy danych i zapisuje je na legitymacji.

Komunikuje się z kartą za pomocą poleceń APDU opisanych normą ISO/IEC 8716-4

Karta musi być przygotowana do bezpośredniej współpracy z systemem Zamawiającego (wykorzystującego platformę JavaCard) poprzez dedykowane polecenia APDU umożliwiające tworzenie, usuwanie i nadpisywanie katalogów i plików w strukturze układu procesorowego.

2. Wykonawca zobowiązany jest wskazać okres gwarancji na dostarczany asortyment, nie krótszy niż 24 miesiące.

FUNKCJONALNOŚCI DODATKOWE

- Oprogramowanie umożliwiające wykorzystanie dodatkowych funkcjonalności karty (tj. dodatkowe zarządzanie kartą i jej testowanie dla systemu Microsoft Windows, korzystanie z funkcjonalności Global Platform: instalowanie i usuwanie apletów, tworzenie/usuwanie/zmiana kluczy, inne)
- Zarządzanie kodem PIN, PUK, inicjowanie karty
- Zarządzanie certyfikatami oraz funkcjonalnością PKI (import, eksport certyfikatu, wskazanie certyfikatu domyślnego, wyświetlanie atrybutów certyfikatu, usunięcie certyfikatu, zarejestrowanie certyfikatu w systemie),
- Logowanie do systemu (domeny) MS Windows, blokowanie i odblokowywanie komputera,
- Podpisywanie dokumentów oraz poczty elektronicznej.