# Załącznik nr 1 do SIWZ

# SPECYFIKACJA TECHNICZNA - OPIS RZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest sukcesywna dostawa blankietów do Elektronicznej Legitymacji Studenckiej o następujących parametrach:

1. **Elektroniczna Legitymacja Studencka (ELS)** zgodnie z załącznikiem nr 1 do Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 27 września 2018 r. w sprawie studiów (Dz. U. z 2018 r. poz. 1861).
2. **Dostawca karty udostępnia nieodpłatnie w ciągu tygodnia po podpisaniu umowy środowisko umożliwiające programowanie karty (SDK-Software Development Kit, biblioteki, gotowe oprogramowanie) wraz z dokumentacją w języku polskim.**

**3. Karta procesorowa – charakterystyka podstawowa**

Wstępnie zadrukowany blankiet ELS (zwany dalej Kartą) jest hybrydową elektroniczną kartą procesorową z dwoma niezależnymi układami procesorowymi: jeden z interfejsem stykowym a drugi z interfejsem bezstykowym:

1. stykowym określonym w normach ISO/IEC 7816-2 i ISO/IEC 7816-3 o pojemności pamięci EEPROM co najmniej 67 kilobajtów
2. bezstykowym określonym w normie 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).

Karty muszą być wykonane z materiału nie ulegającemu odkształceniu i/lub rozwarstwieniu. Białe pole po stronie rewersowej winno być położone w stosunku do brzegów karty z niedokładnością +/- 0,5mm.
Blankiety nie mogą być wygięte, zniekształcone, porysowane oraz sklejone.
Laminat po obydwu stronach karty winien płynnie przykrywać wszystkie zniekształcenia powierzchni zwłaszcza w miejscu wprasowywania chipów.

Sposób wykonania kart określa załącznik nr 1 do Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 27 września 2018 r. w sprawie dokumentacji przebiegu studiów (Dz. U. z 2018 r. poz. 1861).

**KARTA ELS**

Dodatkowy nadruk cyfrowego numeru Mifare oraz kodu kreskowego przewidziany jest w białym polu po stronie rewersowej **karty ELS**. Format nadruku numeru karty:
- zawsze 11 cyfr zgrupowanych w dwóch ciągach rozdzielonych odstępem odpowiednio po 3 i 8 cyfr (np. 001 00000001),

- grupa 3 pierwszych cyfr jest reprezentowana przez czwarty bajt w bloku (bajt nr 3), przyjmuje wartości z przedziału < 000, 255 >,
- grupa pozostałych 8 cyfr jest reprezentowana przez pierwsze trzy bajty w bloku (kolejno bajt nr 2, bajt nr 1, bajt nr 0), przyjmuje wartości z przedziału < 00000000,16777215 >,- obowiązuje zasada uzupełniania każdej grupy cyfr nieznaczącymi zerami (z przodu) do osiągnięcia odpowiednio 3 i 8 cyfr (w sumie zawsze 11 cyfr),
- kod kreskowy w standardzie 128B

**4. Wygląd legitymacji**

1.Wygląd **blankietu ELS** określa załącznik nr 1 do Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 27 września 2018 r. w sprawie dokumentacji przebiegu studiów (Dz. U. z 2018 r poz. 1861)

**5. Część elektroniczna - stykowa**

Część stykowa karty jest wyposażona w interfejs określony w normach ISO/IEC 7816-2 i ISO/IEC 7816-3.

Polecenia i odpowiedzi przesyłane podczas komunikacji Karty z infrastrukturą informatyczną powinny mieć strukturę zgodną z APDU określoną w normie ISO/IEC 7816-4.

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.

Blankiet ELS może być stosowany jako komponent techniczny urządzenia do składania podpisu elektronicznego (ustawa z dnia 18 września 2001 r. o podpisie elektronicznym – Dz. U. 2001 nr 130 poz. 1450).

**6. Blankiet ELS musi spełniać następujące wymagania:**

1. Układ elektroniczny o pojemności pamięci EEPROM co najmniej 67 kilobajtów z wbudowanym koprocesorem kryptograficznym.
2. Pojemność karty dla danych w systemie plików zgodnym z ISO 7816-4 powinna wynosić co najmniej 10KB (kilobajtów).
3. Układ elektroniczny blankietu ELS musi posiadać certyfikat Common Criteria Standard na poziomie co najmniej EAL4+ lub równoważny.
4. Card Management i API zgodne z Global Platform 2.1.1
5. System operacyjny Java Card Virtual Machine, RTE i API zgodne z JC2.2.1
6. Blankiety muszą posiadać certyfikat Common Criteria Standard według profilu PPSSCD Protection Profile – Secure Signature Creation Device Type 2 and/or 3, version 1.05, EAL4+ (CWA14169).
7. Zgodny ze standardem funkcjonalności E-Sign K (CWA14890).
8. DAP zgodne z Global Platform 2.1 (PK-Based).
9. Obsługiwane protokoły: T=0, T=1, PPS.
10. Prędkość transmisji czytnik – karta do 230 Kbauds.
11. Dostęp do klucza prywatnego zapisanego na Karcie możliwy jest wyłącznie przez koprocesor kryptograficzny Karty.
12. Wszystkie operacje kryptograficzne dotyczące klucza prywatnego wykonywane są na karcie.

13. Użycie klucza prywatnego tylko po podaniu kodu PIN użytkownika.
14. 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.
15. 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.

**7. Część elektroniczna – bezstykowa**

Część bezstykowa jest wyposażona w interfejs zgodny z ISO/IEC 14443 typ A.
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 opcjonalnie ISO/IEC 14443-4 (protokół T=CL), przy zachowaniu pełnej antykolizyjności.
Podstawowe parametry techniczne interfejsu bezstykowego:
Pamięć i funkcje logiczne (moduł Mifare®):

| | |
|---|---|
| Pamięć | 8 kBit EEPROM<br>(16 niezależnych sektorów po 4 bloki każdy. Każdy blok o wielkości 16 bajtów) |
| Security block | blok systemowy dla każdego sektora wskazujący prawa dostępu i zawierający 2 klucze 48 bitowe |
| Identyfikacja karty | Niezmienny numer seryjny i inne dane programowalne w pierwszym bloku danych |
| Antykolizyjność | Obsługa wielu kart w polu czytnika, niezależne adresowanie każdej karty |
| Aplikacje - cechy | Struktura elektronicznej portmonetki, niezależne prawa debetowe i kredytowe |
| Protokół komunikacyjny: | half duplex wraz z handshake |
| Szybkość transakcji | |
| Wybór karty z antykolizją | 3 ms |
| Wspólne uwierzytelnienie | 2 ms |
| Odczyt bloku: | 2.5 ms |
| Zapis bloku: | 9 ms |
| Ilość cykli odczytu | Nielimitowana |
| Ilość cykli zapisu | Co najmniej 100 000 cykli |
| Okres przechowywania danych | Co najmniej 10 lat |
| Komunikacja | Częstotliwość nośna 13.56 MHz |

| | |
|---|---|
| Zasilanie | Indukcja magnetyczna |
| Modulacja kodowanie | Zgodna z ISO14443-2 type A |
| Szybkość komunikacji | 106 kbaud |
| Integralność przesyłanych | |
| Danych | CRC16 i Parity bit |
| Zasięg operacyjny | od 0 do 10 cm |

**8. Zabezpieczenia na czas dostawy**

Dostęp do układów elektronicznych blankietów ELS jest zabezpieczany na czas dostawy specjalnymi kluczami transportowymi dla części bezstykowej (MIFARE®) i stykowej.

**9. Oprogramowanie**

Do każdej karty oferent dołączy licencję na oprogramowanie Middleware umożliwiające zarządzanie kartą oraz wykorzystanie dodatkowych możliwości karty.

## 10. Rodzaj karty

Oferowana karta musi być kompatybilna z Systemem USOS. Wykonawca musi podać dokładną nazwę/model oferowanej karty. Zamawiający na tej podstawie będzie weryfikował czy dana karta znajduje się na oficjalnej liście obsługiwanych kart przez system USOS (http://muci.edu.pl/pliki/ELS-USOS.pdf). Niniejsza lista uwzględnia oficjalne wersje/dystrybucje systemu USOS.