

## OPIS PRZEDMIOTU ZAMÓWIENIA

**Specyfikacja dla zakupu 3000 szt. blankietów kart elektronicznej legitymacji studenckiej (ELS) i taśmy kolorowej z overlay'em.****1. Wymagania formalne**

- 1.1.1. Złożenie oświadczenia o zgodności dostarczonych blankietów kart procesorowych z załącznikiem numer 1 Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 16.04.2019 roku w sprawie studiów (Dz. U. 2019 poz. 787) z późniejszymi zmianami.

**2. Wymagania dla 3000 kart procesorowych dostarczonych do współpracy z Systemem Elektronicznej Legitymacji Studenckiej firmy OPTeam S.A.****2.1. Ogólne wymagania dla kart procesorowych**

- 2.1.1. Rodzaj blankietu i wygląd elektronicznej legitymacji studenckiej musi być zgodny z załącznikiem numer 1 Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 16.04.2019 roku w sprawie studiów (Dz. U. 2019 poz. 787) z późniejszymi zmianami.

- 2.1.2. Karty wykonane są z materiału nie ulegającemu odkształceniu i/lub rozwarstwieniu. Sposób wykonania kart określa załącznik numer 1 Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 16.04.2019 roku w sprawie studiów (Dz. U. 2019 poz. 787) z późniejszymi zmianami.

**2.2. Minimalne wymagania techniczne dla kart procesorowych**

Wstępnie zadrukowany blankiet ELS (Karta) elektronicznej legitymacji studenckiej jest hybrydową elektroniczną kartą procesorową z dwoma interfejsami (dwoma, niezależnymi układami elektronicznymi).

- 2.2.1. Karta procesorowa musi być kartą hybrydową.

- 2.2.2. Interfejs stykowy musi być zgodny z normami ISO/IEC 7816-2 i ISO/IEC 7816-3 o pojemności pamięci EEPROM co najmniej 75 kilobajtów.

- 2.2.3. Interfejs bezstykowy musi być zgodny z normą ISO/IEC 14443 typ A, zgodnym ze standardem przemysłowym MIFARE® DESFIRE EV1 o pojemności pamięci 4 kilobajty (MIFARE® DESFire EV1 4k - MF3 IC D41).

- 2.2.4. Wymagania dla części elektronicznej – stykowej.

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

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

- 2.2.4.3. Polecenia realizowane przez Kartę dla operacji kryptograficznych i zarządzania są zgodne z ISO/IEC 7816-8, ISO/IEC 7816-9.

- 2.2.4.4. Blankiet ELS musi spełniać następujące wymagania:

- 2.2.4.5. Układ elektroniczny o pojemności pamięci EEPROM co najmniej 75 kilobajtów z wbudowanym koprocesorem kryptograficznym.

- 2.2.4.6. Układ elektroniczny blankietu ELS musi posiadać certyfikat Common Criteria Standard na poziomie co najmniej EAL5+.

- 2.2.4.7. Card Management i API zgodne z Global Platform 2.1.1

- 2.2.4.8. System operacyjny Java Card Virtual Machine, RTE i API zgodne z JC2.2.2 wraz z rozszerzeniami JC 3.0 o wsparcie dla kryptografii bazującej na krzywych eliptycznych (ECC).

- 2.2.4.9. Blankiet ELS musi posiadać certyfikat Common Criteria Standard na poziomie co najmniej EAL5+ według profilu PP SSCD/QSCD Protection Profile – Qualified Signature Creation Device/Secure Signature Creation Device wg EN 419211 część 1 do 6 (poprzednio publikowane pod kodem EN 14169). Zgodność ze specyfikacją eIDAS.

- 2.2.4.10. Zgodny ze standardem funkcjonalności E-Sign K (CWA14890).

- 2.2.4.11. DAP zgodne z Global Platform 2.1.1 (PK-Based).

- 2.2.4.12. Funkcjonalność PKI zgodna ze standardem minidriver ver. 7.x firmy Microsoft oraz PKCS#11 ver. 2.20. Minidriver dla karty powinien być dostępny na stronach Microsoft Update.

- 2.2.4.13. Obsługiwane protokoły: T=0, T=1, PPS.

- 2.2.4.14. Prędkość transmisji czytnik – karta do 230 Kbauds.

- 2.2.4.15. Dostęp do klucza prywatnego zapisanego na Karcie możliwy jest wyłącznie przez koprocesor kryptograficzny Karty.

- 2.2.4.16. Wszystkie operacje kryptograficzne dotyczące klucza prywatnego wykonywane na karcie.

- 2.2.4.17. Użycie klucza prywatnego tylko po podaniu kodu PIN użytkownika. Osobna para PIN/PUK dla kluczy związanych z kwalifikowanym certyfikatem.

- 2.2.4.18. Blankiet ELS w części stykowej musi pozwalać na zarządzanie pamięcią EEPROM poprzez: usuwanie apletów/pakietów, udostępnianie pamięci zwolnionej po usunięciu apletu/pakietu i defragmentację luk w pamięci EEPROM.
- 2.2.4.19. Generowanie kluczy kryptograficznych o długości do 2048 bitów przeznaczonych do użycia przez algorytm RSA, podpisywanie za pomocą algorytmu RSA. Generowanie kluczy kryptograficznych ECC o długości do 521 bitów, podpisywanie za pomocą algorytmu ECC, obsługa funkcji skrótu SHA-1, SHA-256, SHA-384, SHA-512, obsługa algorytmów 3DES (ECB, CBC), AES (128, 192, 256 bitów).
- 2.2.4.20. 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.
- 2.2.5. Wymagania dla części elektronicznej – bezstykowej
- 2.2.5.1. Część bezstykowa jest wyposażona w interfejs zgodny z ISO/IEC 14443 typ A.
  - 2.2.5.2. Sposób komunikacji karty jest zgodny ze standardem przemysłowym MIFARE® DESFIRE
  - 2.2.5.3. Pamięć: EEPROM 4kB
  - 2.2.5.4. Organizacja pamięci - System plików
  - 2.2.5.5. Ilość cykli zapisów: 500 000
  - 2.2.5.6. Interfejs RF: Typ: ISO 14443 1-4
  - 2.2.5.7. Prędkość transmisji: 106-848 kbit/s
  - 2.2.5.8. Zasięg działania: do 10 cm
  - 2.2.5.9. Wbudowany generator liczb losowych
  - 2.2.5.10. Wieloaplikacyjność: 28 aplikacji, MAD3
  - 2.2.5.11. Unikalny numer seryjny: 7B
  - 2.2.5.12. Zaimplementowane mechanizmy kryptograficzne: DES, DES3, AES(128bit) 3KDES

#### 2.2.6. Zabezpieczenia na czas dostawy

Dostęp do układów elektronicznych blankietów ELS (Elektronicznej Legitymacji Studenckiej) jest zabezpieczony na czas dostawy specjalnymi kluczami transportowymi dla części bezstykowej (MIFARE® DESFIRE) i stykowej. Klucze transportowe dla części bezstykowej muszą być akceptowane przez Zarząd Transportu Miejskiego w Kielcach (ul. Głowackiego 4; 25-368 Kielce ) w związku z możliwością wykorzystania legitymacji studenckiej jako Kieleckiej Karty Miejskiej w Kielcach.

#### 2.2.7. Oprogramowanie

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

2.2.8. Karta musi współpracować z Systemem Elektronicznej Legitymacji Studenckiej OPTIcamp firmy OPTeam S.A. (OPTeam S.A. ul. Tajęcina 113, 36-002 Jasionka) zaimplementowanym w Uniwersytecie Jana Kochanowskiego w Kielcach.

### **Warunki gwarancji**

**Gwarancja co najmniej 12 miesięcy i 24 m-ce rękojmi**

**Nieodpłatna wymiana wadliwych kart na pozbawione wad karty.**

### **3. Wymagania dla materiałów eksploatacyjnych do drukarki kart Evolis Primacy**

3.1. Taśmy kolorowe z overlay'em w ilości umożliwiającej wydrukowanie dwustronne 1500 (tysiąc pięćset sztuk) kart. Ilość taśm – 10 sztuk. Obydwie strony karty pokrywane są warstwą zabezpieczającą overlay;

3.1.1. Opis taśmy do drukarki Dualis Primacy : YMCKO 5 Panel Color Ribbon, P/N : R5F008EAA, 300 cards /roll;

### **Gwarancja na materiały eksploatacyjne 12 miesięcy i rękojmi 24 m-ce**

#### **Specyfikacja dla zakupu 50 szt. blankietów kart elektronicznej legitymacji doktoranta (ELD)**

##### **Wymagania formalne**

3.1.2. Złożenie oświadczenia o zgodności dostarczonych blankietów kart procesorowych z Rozporządzeniem Ministra Nauki i Szkolnictwa Wyższego z dnia 21 września 2018 roku w sprawie dyplomów doktorskich, dyplomów habilitacyjnych i legitymacji doktoranta (Dz. U. 2018 poz. 1837) z późniejszymi zmianami oraz Ustawą z dnia 13 stycznia 2023 r. o zmianie ustawy - Prawo o szkolnictwie wyższym i nauce oraz niektórych innych ustaw (Dz. U.2023 poz.212)

### **4. Wymagania dla 50 kart procesorowych dostarczonych do współpracy z Systemem Elektronicznej Legitymacji Doktoranta firmy OPTeam S.A.**

#### **4.1. Ogólne wymagania dla kart procesorowych**

- 4.1.1. Rodzaj blankietu i wygląd elektronicznej legitymacji doktoranta musi być zgodny z Rozporządzeniem Ministra Nauki i Szkolnictwa Wyższego z dnia 21 września 2018 roku w sprawie dyplomów doktorskich, dyplomów habilitacyjnych i legitymacji doktoranta (Dz. U. 2018 poz. 1837) z późniejszymi zmianami oraz Ustawą z dnia 13 stycznia 2023 r. o zmianie ustawy - Prawo o szkolnictwie wyższym i nauce oraz niektórych innych ustaw (Dz. U.2023 poz.212)
- 4.1.2. Karty wykonane są z materiału nie ulegającemu odkształceniu i / lub rozwarstwieniu. Sposób wykonania kart określa Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 21 września 2018 roku w sprawie dyplomów doktorskich, dyplomów habilitacyjnych i legitymacji doktoranta (Dz. U. 2018 poz. 1837) z późniejszymi zmianami oraz Ustawą z dnia 13 stycznia 2023 r. o zmianie ustawy - Prawo o szkolnictwie wyższym i nauce oraz niektórych innych ustaw (Dz. U.2023 poz.212)

#### 4.2. Minimalne wymagania techniczne dla kart procesorowych

Wstępnie zadrukowany blankiet ELD (Karta) elektronicznej legitymacji doktoranta jest hybrydową elektroniczną kartą procesorową z dwoma interfejsami (dwoma, niezależnymi układami elektronicznymi).

- 4.2.1. Karta procesorowa musi być kartą hybrydową.
- 4.2.2. Interfejs stykowy musi być zgodny z normami ISO/IEC 7816-2 i ISO/IEC 7816-3 o pojemności pamięci EEPROM co najmniej 75 kilobajtów.
- 4.2.3. Interfejs bezstykowy musi być zgodny z normą ISO/IEC 14443 typ A, zgodnym ze standardem przemysłowym MIFARE® DESFIRE EV1 o pojemności pamięci 4 kilobajty (MIFARE® DESFire EV1 4k - MF3 IC D41).
- 4.2.4. Wymagania dla części elektronicznej – stykowej.
  - 4.2.4.1. Część stykowa karty jest wyposażona w interfejs określony w normach ISO/IEC 7816-2 i ISO/IEC 7816-3.
  - 4.2.4.2. Polecenia i odpowiedzi przesyłane podczas komunikacji Karty z infrastrukturą informatyczną powinny mieć strukturę zgodną z APDU określoną w normie ISO/IEC 7816-4.
  - 4.2.4.3. Polecenia realizowane przez Kartę dla operacji kryptograficznych i zarządzania są zgodne z ISO/IEC 7816-8, ISO/IEC 7816-9.
  - 4.2.4.4. Blankiet ELD musi spełniać następujące wymagania:
  - 4.2.4.5. Układ elektroniczny o pojemności pamięci EEPROM co najmniej 75 kilobajtów z wbudowanym koprocesorem kryptograficznym.
  - 4.2.4.6. Układ elektroniczny blankietu ELS musi posiadać certyfikat Common Criteria Standard na poziomie co najmniej EAL5+.
  - 4.2.4.7. Card Management i API zgodne z Global Platform 2.1.1
  - 4.2.4.8. System operacyjny Java Card Virtual Machine, RTE i API zgodne z JC2.2.2 wraz z rozszerzeniami JC 3.0 o wsparcie dla kryptografii bazującej na krzywych eliptycznych (ECC).
  - 4.2.4.9. Blankiet ELD musi posiadać certyfikat Common Criteria Standard na poziomie co najmniej EAL5+ według profilu PP SSCD/QSCD Protection Profile – Qualified Signature Creation Device/Secure Signature Creation Device wg EN 419211 część 1 do 6 (poprzednio publikowane pod kodem EN 14169). Zgodność ze specyfikacją eIDAS.
  - 4.2.4.10. Zgodny ze standardem funkcjonalności E-Sign K (CWA14890).
  - 4.2.4.11. DAP zgodne z Global Platform 2.1.1 (PK-Based).
  - 4.2.4.12. Funkcjonalność PKI zgodna ze standardem minidriver ver. 7.x firmy Microsoft oraz PKCS#11 ver. 2.20. Minidriver dla karty powinien być dostępny na stronach Microsoft Update.
  - 4.2.4.13. Obsługiwane protokoły: T=0, T=1, PPS.
  - 4.2.4.14. Prędkość transmisji czytnik – karta do 230 Kbauds.
  - 4.2.4.15. Dostęp do klucza prywatnego zapisanego na Karcie możliwy jest wyłącznie przez koprocesor kryptograficzny Karty.
  - 4.2.4.16. Wszystkie operacje kryptograficzne dotyczące klucza prywatnego wykonywane na karcie.
  - 4.2.4.17. Użycie klucza prywatnego tylko po podaniu kodu PIN użytkownika. Osobna para PIN/PUK dla kluczy związanych z kwalifikowanym certyfikatem.
  - 4.2.4.18. Blankiet ELD w części stykowej musi pozwalać na zarządzanie pamięcią EEPROM poprzez: usuwanie apletów/pakietów, udostępnianie pamięci zwolnionej po usunięciu apletu/pakietu i defragmentację luk w pamięci EEPROM.
  - 4.2.4.19. Generowanie kluczy kryptograficznych o długości do 2048 bitów przeznaczonych do użycia przez algorytm RSA, podpisywanie za pomocą algorytmu RSA. Generowanie kluczy kryptograficznych ECC o długości do 521 bitów, podpisywanie za pomocą algorytmu ECC, obsługa funkcji skrótu SHA-1, SHA-256, SHA-384, SHA-512, obsługa algorytmów 3DES (ECB, CBC), AES (128, 192, 256 bitów)

4.2.4.20. 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.

4.2.5. Wymagania dla części elektronicznej – bezstykowej

- 4.2.5.1. Część bezstykowa jest wyposażona w interfejs zgodny z ISO/IEC 14443 typ A.
- 4.2.5.2. Sposób komunikacji karty jest zgodny ze standardem przemysłowym MIFARE® DESFIRE
- 4.2.5.3. Pamięć: EEPROM 4kB
- 4.2.5.4. Organizacja pamięci - System plików
- 4.2.5.5. Ilość cykli zapisów: 500 000
- 4.2.5.6. Interfejs RF: Typ: ISO 14443 1-4
- 4.2.5.7. Prędkość transmisji: 106-848 kbit/s
- 4.2.5.8. Zasięg działania: do 10 cm
- 4.2.5.9. Wbudowany generator liczb losowych
- 4.2.5.10. Wieloaplikacyjność: 28 aplikacji, MAD3
- 4.2.5.11. Unikalny numer seryjny: 7B
- 4.2.5.12. Zaimplementowane mechanizmy kryptograficzne: DES, DES3, AES(128bit) 3KDES

4.2.6. Zabezpieczenia na czas dostawy

Dostęp do układów elektronicznych blankietów ELD (Elektronicznej Legitymacji Doktoranta) jest zabezpieczany na czas dostawy specjalnymi kluczami transportowymi dla części bezstykowej (MIFARE® DESFIRE) i stykowej. Klucze transportowe dla części bezstykowej muszą być akceptowane przez Zarząd Transportu Miejskiego w Kielcach (ul. Głowackiego 4; 25-368 Kielce ) w związku z możliwością wykorzystania legitymacji doktoranta jako Kieleckiej Karty Miejskiej w Kielcach.

4.2.7. Oprogramowanie

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

4.2.8. Karta musi współpracować z Systemem Elektronicznej Legitymacji Doktoranta OPTIcamp firmy OPTeam S.A. (OPTeam S.A. ul. Tajęcina 113, 36-002 Jasionka) zaimplementowanym w Uniwersytecie Jana Kochanowskiego w Kielcach.

#### **Warunki gwarancji**

**Gwarancja co najmniej 12 miesięcy i 24 m-ce rękojmi.**

**Nieodpłatna wymiana wadliwych kart na pozbawione wad karty.**