Szczegółowy opis przedmiotu zamówienia do części 5

Przedmiotem zamówienia są drukarki do blankietów kart ELS, ELD i pracowniczych (elementy systemu personalizacji oraz kontroli dostępu). Zakup realizowany jest w ramach dofinansowanego projektu POWER „Zintegrowany Program Rozwoju Uczelni".

Drukarki będę integrowane z posiadanymi lub wdrażanymi przez Zamawiającego systemami:

- OptiCamp Perso, systemem personalizacji kart ELS, EKD i EKP, obecnie używanym na Uczelni

- USOS, systemem zarządzania uczelnią, systemem wdrażanym w ramach tego samego projektu.

Dostawca drukarki zobowiązany jest do :

- konfiguracji urządzeń na stanowisku Zamawiającego
- przeprowadzenie testów sprawdzających wydruk i funkcje sprzętu na próbkach kart dostarczonych przez Zamawiającego

2. Drukarka blankietów ELS, ELD, EKP – 2 szt (CPV-30232000-4)

Specyfikacja - w ofercie należy podać specyfikację do porównania	
Rodzaj druku	Kolor i monochromatyczny
Typ nadruku	Jednostronny i dwustronny
Prędkość druku	Min 210 w druku kolorowym jednostronnym, min 120 w druku kolorowym dwustronnym – na godzine
Rozdzielczość	Standardowa 300x300 dpi, rozszerzona dla druku kolorowego do 600x300dpi oraz 300x1200dpi dla druku mono
Obsługa kart	Co najmniej PCV, kompozytowe PCV, PET, wg ISO CR80-ISO 7810, grubość 0,25 do 1,25 mm
Kodery (dołączone)	Koder kart stykowych, koder kart zbliżeniowych MIFARE
Porty	USB, Ethernet

Laminarka	Zainstalowana w drukarce
Podajnik	Min 100 kart
Odbiornik kart odrzuconych	Min 30 kart
Obsługiwane grubości kart	0,25 – 1,25 mm (10-50 mil)
Inne	Wykonawca powinien dostarczyć materiały eksploatacyjne niezbędne do wydruku 250 szt. kart dwustronnie w kolorze. Oprogramowanie i instrukcja dostępne w języku polskim.
Kompatybilność	Drukarka musi być kompatybilna z systemami operacyjnymi • Windows *32/64 bits) XP SP3, Vista, W7,W8,W10 • Mac OS X (od wersji 10,5)
Gwarancja	Min. 3 lata

3. Blankiety ELS (CPV- 30162000-2)

	ELS – Elektroniczna Legitymacja Studenta
1.	Zamawiający wymaga dostawy 150 szt. blankietów ELS
2.	Wstępnie zadrukowany blankiet ELS (Karta) musi być hybrydową elektroniczną kartą procesorową z dwoma interfejsami (dwoma, niezależnymi układami elektronicznymi): • stykowym określonym w normach ISO/IEC 7816-2 i ISO/IEC 7816-3 o pojemności pamięci EEPROM co najmniej 75 kilobajtów • 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 lub równowazny). Karty wykonane są z materiału nie ulegającemu odkształceniu i / lub rozwarstwieniu. Sposób wykonania kart określa Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego.
3.	ELS musi być wykonana z materiału nie ulegającemu odkształceniu i / lub rozwarstwieniu.
4.	ELS musi umożliwiać zastosowanie jako kwalifikowane urządzenie do składania podpisu elektronicznego zgodnie z wymogami Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR

	910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE – Załącznik II Wymogi dla kwalifikowanych urządzeń do składania podpisu elektronicznego -, na które powołuje się Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016 poz. 1579).
5.	Wygląd blankietu ELS określa Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 29 września 2018 r. w sprawie studiów.
6.	Część stykowa ELS musi być wyposażona w interfejs określony w normach ISO/IEC 7816-2 i ISO/IEC 7816-3.
7.	Polecenia i odpowiedzi przesyłane podczas komunikacji ELS z infrastrukturą informatyczną powinny mieć strukturę zgodną z APDU określoną w normie ISO/IEC 7816-4.
8.	Polecenia realizowane przez ELS dla operacji kryptograficznych i zarządzania muszą być zgodne z ISO/IEC 7816-8, ISO/IEC 7816-9.
9.	Blankiet ELS musi spełniać następujące wymagania: • układ elektroniczny o pojemności pamięci EEPROM co najmniej 75 kilobajtów z wbudowanym koprocesorem kryptograficznym. • układ elektroniczny blankietu ELS musi posiadać certyfikat Common Criteria Standard na poziomie co najmniej EAL5+. • Card Management i API zgodne z Global Platform 2.1.1 • system operacyjny Java Card Virtual Machine, RTE i API zgodne z JC2.2.2 wraz z roszerzeniami JC 3.0 o wsparcie dla kryptografii bazującej na krzywych eliptycznych (ECC) • 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. • zgodość ze standardem funkcjonalności E-Sign K (CWA14890). • DAP zgodne z Global Platform 2.1.1 (PK-Based). • 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. • obsługiwane protokoły: T=0, T=1, PPS. • prędkość transmisji czytnik – karta do 230 Kbauds. • dostęp do klucza prywatnego zapisanego na Karcie możliwy jest wyłącznie przez procesor kryptograficzny Karty. • wszystkie operacje kryptograficzne dotyczące klucza prywatnego wykonywane na karcie. • użycie klucza prywatnego tylko po podaniu kodu PIN użytkownika. Osobna para PIN/PUK dla kluczy związanych z kwalifikowanym certyfikatem.

	• 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. • 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). • 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.
10.	Część bezstykowa ELS musi być wyposażona w interfejs zgodny z ISO/IEC 14443 typ A.
11.	Sposób komunikacji ELS musi być 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.
12.	Dostęp do układów elektronicznych blankietów ELS musi być zabezpieczany na czas dostawy specjalnymi kluczami transportowymi dla części bezstykowej (MIFARE®) i stykowej.
13.	Proponowane Karty muszą być zgodne (kompatybilne) z systemem personalizacji kart elektronicznych wykorzystywanym przez Zamawiającego

4. Blankiety ELD (CPV- 30162000-2)

	ELD – Elektroniczna Legitymacja Doktoranta
14.	Zamawiający wymaga dostawy 30 szt. blankietów ELD
15.	Wstępnie zadrukowany blankiet ELD (Karta) musi być hybrydową elektroniczną kartą procesorową z dwoma interfejsami (dwoma, niezależnymi układami elektronicznymi): • stykowym określonym w normach ISO/IEC 7816-2 i ISO/IEC 7816-3 o pojemności pamięci EEPROM co najmniej 75 kilobajtów • 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 lub równowazny). Karty wykonane są z materiału nie ulegającemu odkształceniu i / lub rozwarstwieniu. Sposób wykonania kart określa Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego.

16.	ELD musi być wykonana z materiału nie ulegającemu odkształceniu i / lub rozwarstwieniu.
17.	ELD musi umożliwiać zastosowanie jako kwalifikowane urządzenie do składania podpisu elektronicznego zgodnie z wymogami Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE – Załącznik II Wymogi dla kwalifikowanych urządzeń do składania podpisu elektronicznego -, na które powołuje się Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016 poz. 1579).
18.	Wygląd blankietu ELD określa Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 29 września 2018 r. w sprawie studiów.
19.	Część stykowa ELD musi być wyposażona w interfejs określony w normach ISO/IEC 7816-2 i ISO/IEC 7816-3.
20.	Polecenia i odpowiedzi przesyłane podczas komunikacji ELD z infrastrukturą informatyczną powinny mieć strukturę zgodną z APDU określoną w normie ISO/IEC 7816-4.
21.	Polecenia realizowane przez ELD dla operacji kryptograficznych i zarządzania muszą być zgodne z ISO/IEC 7816-8, ISO/IEC 7816-9.
22.	Blankiet ELD musi spełniać następujące wymagania: • układ elektroniczny o pojemności pamięci EEPROM co najmniej 75 kilobajtów z wbudowanym koprocesorem kryptograficznym. • układ elektroniczny blankietu ELD musi posiadać certyfikat Common Criteria Standard na poziomie co najmniej EAL5+. • Card Management i API zgodne z Global Platform 2.1.1 • system operacyjny Java Card Virtual Machine, RTE i API zgodne z JC2.2.2 wraz z roszerzeniami JC 3.0 o wsparcie dla kryptografii bazującej na krzywych eliptycznych (ECC) • 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. • zgodość ze standardem funkcjonalności E-Sign K (CWA14890). • DAP zgodne z Global Platform 2.1.1 (PK-Based). • 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. • obsługiwane protokoły: T=0, T=1, PPS. • prędkość transmisji czytnik – karta do 230 Kbauds. • dostęp do klucza prywatnego zapisanego na Karcie możliwy jest wyłącznie przez procesor kryptograficzny Karty. • wszystkie operacje kryptograficzne dotyczące klucza prywatnego wykonywane na karcie.

	• użycie klucza prywatnego tylko po podaniu kodu PIN użytkownika. Osobna para PIN/PUK dla kluczy związanych z kwalifikowanym certyfikatem. • 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. • 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). • 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.
23.	Część bezstykowa ELD musi być wyposażona w interfejs zgodny z ISO/IEC 14443 typ A.
24.	Sposób komunikacji ELD musi być 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.
25.	Dostęp do układów elektronicznych blankietów ELD musi być zabezpieczany na czas dostawy specjalnymi kluczami transportowymi dla części bezstykowej (MIFARE®) i stykowej.
26.	Proponowane Karty muszą być zgodne (kompatybilne) z systemem personalizacji kart elektronicznych wykorzystywanym przez Zamawiającego

5. Blankiety EKP (CPV- 30162000-2)

	EKP – Elektroniczna Karta Pracownika
1.	Zamawiający wymaga dostawy 50 szt. blankietów EKP
2.	Blankiet EKP musi być hybrydową elektroniczną kartą procesorową z dwoma interfejsami (dwoma, niezależnymi układami elektronicznymi): • stykowym określonym w normach ISO/IEC 7816-2 i ISO/IEC 7816-3 o pojemności pamięci EEPROM co najmniej 75 kilobajtów • 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 lub równowazny).

3.	EKP musi być wykonana z materiału nie ulegającemu odkształceniu i / lub rozwarstwieniu.
4.	EKP musi umożliwiać zastosowanie jako kwalifikowane urządzenie do składania podpisu elektronicznego zgodnie z wymogami Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE – Załącznik II Wymogi dla kwalifikowanych urządzeń do składania podpisu elektronicznego -, na które powołuje się Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016 poz. 1579).
5.	EKP musi umożliwiać nadanie wyglądu (personalizacja graficzna) określonego przez Uczelnię.
6.	Część stykowa EKP musi być wyposażona w interfejs określony w normach ISO/IEC 7816-2 i ISO/IEC 7816-3.
7.	Polecenia i odpowiedzi przesyłane podczas komunikacji EKP z infrastrukturą informatyczną powinny mieć strukturę zgodną z APDU określoną w normie ISO/IEC 7816-4.
8.	Polecenia realizowane przez EKP dla operacji kryptograficznych i zarządzania muszą być zgodne z ISO/IEC 7816-8, ISO/IEC 7816-9.
9.	Blankiet EKP musi spełniać następujące wymagania: • układ elektroniczny o pojemności pamięci EEPROM co najmniej 75 kilobajtów z wbudowanym koprocesorem kryptograficznym. • układ elektroniczny blankietu EKP musi posiadać certyfikat Common Criteria Standard na poziomie co najmniej EAL5+. • Card Management i API zgodne z Global Platform 2.1.1 • system operacyjny Java Card Virtual Machine, RTE i API zgodne z JC2.2.2 wraz z roszerzeniami JC 3.0 o wsparcie dla kryptografii bazującej na krzywych eliptycznych (ECC) • blankiet EKP 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. • zgodość ze standardem funkcjonalności E-Sign K (CWA14890). • DAP zgodne z Global Platform 2.1.1 (PK-Based). • 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. • obsługiwane protokoły: T=0, T=1, PPS. • prędkość transmisji czytnik – karta do 230 Kbauds. • dostęp do klucza prywatnego zapisanego na Karcie możliwy jest wyłącznie przez procesor kryptograficzny Karty. • wszystkie operacje kryptograficzne dotyczące klucza prywatnego wykonywane na karcie.

	• użycie klucza prywatnego tylko po podaniu kodu PIN użytkownika. Osobna para PIN/PUK dla kluczy związanych z kwalifikowanym certyfikatem. • blankiet EKP 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. • 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). • 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.
10.	Część bezstykowa EKP musi być wyposażona w interfejs zgodny z ISO/IEC 14443 typ A.
11.	Sposób komunikacji EKP musi być 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.
12.	Dostęp do układów elektronicznych blankietów EKP musi być zabezpieczany na czas dostawy specjalnymi kluczami transportowymi dla części bezstykowej (MIFARE®) i stykowej.
13.	Proponowane Karty muszą być zgodne (kompatybilne) z systemem personalizacji kart elektronicznych wykorzystywanym przez Zamawiającego