

Załącznik nr 1 do zapytania ofertowego nr 5/POWR/ZR21/2022

SZCZEGÓŁOWY WYKAZ FUNKCJONALNOŚCI

Wdrożenie samoobsługowego systemu wydawania elektronicznych legitymacji dla studentów Akademii WSB w ramach projektu „EduLider – rozwój Akademii WSB dla regionu”, współfinansowanego ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego, Program Operacyjny Wiedza Edukacja Rozwój 2014-2020, Oś Priorytetowa III. Szkolnictwo wyższe dla gospodarki rozwoju, Działanie 3.5 Kompleksowe programy szkół wyższych.

Dostarczony system musi spełniać wszystkie funkcjonalności wymagane, zawarte w załączniku.

Nazwa proponowanego przez Wykonawcę systemu :

Zastosowanie	System personalizacji ELS, ELD, EKP, LSNA		
I	Wymagania ogólne	W- Wymagane O - Opcjonalne	Tak/Nie
1.	Przygotowanie testów akceptacyjnych wraz z scenariuszami testowymi na potrzeby odbioru zawierające: - testy funkcjonalności zaoferowanego rozwiązania, - testy wydajnościowe przy obciążeniu systemu, - testy weryfikujące poprawność przeniesienia danych z aktualnie wykorzystywanego systemu do zaproponowanego rozwiązania.	W	

2.	Wykonawca przygotuje i przedstawi zamawiającemu analizę wyników przeprowadzonej migracji danych.	W	
3.	Rodzaj licencji – niewyłączna, nieograniczona czasowo, sprzętowo ani terytorialnie, na wszystkie moduły systemu, dla nieograniczonej liczby użytkowników zewnętrznych i wewnętrznych.	W	
4.	System musi być zabezpieczony przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej, w taki sposób, że w razie awarii tracone są jedynie bieżące nie zapisane transakcje.	W	
5.	System musi być zabezpieczony przed dostępem nieuprawnionych osób lub programów.	W	
6.	Natywnym językiem zapytań silnika bazy danych musi być język SQL. System musi umożliwiać instalację na systemach operacyjnych Microsoft Windows Server 2016 lub nowszym, baza danych musi umożliwiać instalację na Microsoft SQL Server w wersji 2017 lub nowszej.	W	
7.	Silnik baz danych musi zapewniać : 1. relacyjność, 2. integralność danych, 3. transakcyjność, 4. skalowalność.	W	

8.	System bazodanowy musi zapewniać dostęp do danych wyłącznie po poprawnym uwierzytelnieniu. Dotyczy to zarówno dostępu przy pomocy programu, jak i wszystkich innych metod dostępu.	W	
9.	System musi umożliwiać definiowanie grup użytkowników oraz nadawanie uprawnień na poziomie grup użytkowników oraz na poziomie pojedynczych użytkowników.	W	
10.	System musi być zabezpieczony przed utratą danych oraz musi zachowywać spójność danych w bazie w przypadku utraty komunikacji w sieci komputerowej.	W	
11.	Nawigacja w systemie musi być zgodna z wymaganiami WCAG 2.0.	W	
12.	Moduł administrowania systemem musi pozwalać na zmianę parametrów jego pracy wykonywaną przez administratora systemu bez interwencji Wykonawcy.	W	
13.	Modyfikowanie wierszy nie może blokować ich odczytu, z kolei odczyt wierszy nie może ich blokować do celów modyfikacji. Jednocześnie spójność odczytu musi gwarantować uzyskanie rezultatów zapytań odzwierciedlających stan danych z chwili jego rozpoczęcia, niezależnie od modyfikacji przeglądanych zbioru danych.	W	

II	Architektura	W- Wymagane O - Opcjonalne	Tak/Nie
14.	System musi być wykonany w technologii trójwarstwowej (warstwa prezentacji/warstwa logiki biznesowej/warstwa bazy danych), a dane muszą być przechowywane w modelu relacyjnym z wykorzystaniem transakcyjnego serwera bazy danych.	W	
II	Wymagania techniczne	W- Wymagane O - Opcjonalne	Tak/Nie
15.	System musi umożliwiać aktualizację z zachowaniem środków bezpieczeństwa przed utratą danych.	W	
16.	System musi umożliwiać stosowanie zestawu znaków narodowych w kodowaniu UTF-8.	W	
17.	Aplikacyjna część systemu dostępna dla pracowników administracyjnych musi posiadać interfejs w języku polskim.	W	
18.	Internetowa część systemu musi posiadać interfejs minimalnie w językach polskim i angielskim.	W	
19.	System musi posiadać konstrukcję modułową, z możliwością niezależnego, stopniowego uruchamiania poszczególnych funkcjonalności. Jednocześnie system musi stanowić integralną całość.	W	

20.	System musi mieć możliwość udostępniania danych za pomocą usług web services.	W	
21.	System musi być odporny na zawieszenie się stacji roboczych, tj. usterka stacji roboczej w trakcie pracy w systemie nie może spowodować niestabilności pracy systemu dla pozostałych użytkowników.	W	
22.	System u użytkownika końcowego musi pracować w natywnych rozdzielczościach ekranu stacji roboczej.	W	
23.	System musi wizualnie oznaczać w interfejsie użytkownika pola, których uzupełnienie w Systemie jest obligatoryjne.	W	
24.	System będzie umożliwiać eksport danych do pakietu MS Office, wykorzystywanego powszechnie przez Zamawiającego.	W	
25.	System pozwala na pracę zdalną dla użytkowników łączących się z infrastrukturą wewnętrzną za pomocą połączenia VPN.	W	
26.	System będzie posiadać odpowiednie zabezpieczenia uniemożliwiające nieuprawniony użytkownikom dostęp do danych i/lub całej aplikacji.	W	

IV	Dostęp do systemu i jego zasobów	W- Wymagane O - Opcjonalne	Tak/Nie
27.	System musi umożliwiać jednoczesny dostęp do danych przez wielu użytkowników, z ochroną tych danych przed utratą spójności lub zniszczeniem.	W	
28.	System musi posiadać zabezpieczenia danych przed niepowołanym dostępem, dzięki możliwości przydzielania zakresu uprawnień poszczególnym użytkownikom i grupom użytkowników.	W	
29.	System musi zapewniać bezpieczne połączenia sieciowe, uniemożliwiające podsłuchiwanie transmisji. Poziom zabezpieczenia transmisji nie będzie niższy od poziomu zapewnianego przez protokoły SSL wersja 3.0/TLS wersja 1.1 z kluczem o długości 128 bitów.	W	
30.	System musi uniemożliwiać wprowadzanie i modyfikację danych w sposób anonimowy.	W	
31.	System musi posiadać zabezpieczenia przed dostępem osób nieautoryzowanych. Zabezpieczenia muszą funkcjonować na poziomie klienta, serwera aplikacji i serwera bazy danych.	W	

V	Zabezpieczenia i przetwarzanie danych	W- Wymagane O - Opcjonalne	Tak/Nie
32.	Dane gromadzone w systemie przetwarzane mogą być na serwerach uczelni, zlokalizowanych w sieci wewnętrznej. Sieć wewnętrzna zapewnia odpowiednie środki ochrony fizycznej danych (np. przechowywanie serwerów w pomieszczeniach zabezpieczonych), środki sprzętowe (np. zasilacze awaryjne) oraz organizacyjne (np. cykliczne wykonywanie kopii bezpieczeństwa danych).	W	
33.	Uwierzytelnianie za pomocą wewnętrznych metod autoryzacji użytkowanych systemów informatycznych.	W	
34.	W systemie muszą zostać wykorzystane następujące mechanizmy zapewnienia bezpieczeństwa danych: 1. logowanie za pomocą sesji, 2. walidacja danych wejściowych na poziomie przeglądarki i serwera; 3. szyfrowanie SSL przy pomocy posiadanego przez Zamawiającego certyfikatu SSL, 4. oprogramowanie antywirusowe serwera (dostarczane przez Zamawiającego), 5. Oprogramowanie do backupu (dostarczane przez Zamawiającego).	W	
35.	W celu zapewnienia bezpieczeństwa przetwarzania danych w systemie muszą zostać zastosowane następujące mechanizmy: 1. Rejestracja zmian - każde działanie użytkownika na danych (dodawania, usuwanie i edytowanie) musi być rejestrowane w systemie,	W	

	2. Dostęp do części niepublicznej systemu mogą mieć tylko upoważnione osoby posiadające unikalny identyfikator i przypisane do niego hasło, każde wejście/wyjście i działania użytkownika w systemie mogą zostać zarejestrowane, 3. Kilkukrotna nieudana próba uzyskania dostępu do systemu musi skutkować zablokowaniem konta, 4. Każdy użytkownik części aplikacyjnej systemu może mieć dostęp do ściśle określonych zasobów systemu sterowany poprzez uprawnienia możliwe do zdefiniowania w systemie, 5. Przetwarzanie danych osobowych będzie się odbywać na warunkach określonych w przepisanych o ochronie danych osobowych.		
VI	Interfejs użytkownika	W- Wymagane O - Opcjonalne	Tak/Nie
36.	System musi: 1. pozwalać na wykorzystywanie bezpiecznego protokołu transmisji/szyfrowania połączeń (SSL z kluczem co najmniej 128 bitów, lub równoważny); 2. zapewniać wsparcie co najmniej dla przeglądarek internetowych: 1) Microsoft Edge 88 lub nowsza, 2) Mozilla Firefox wersja 85 lub nowsza, 3) Safari wersja 14 lub nowsza, 4) Chrome wersja 88 lub nowsza, 5) Opera wersja 73 lub nowsza; 3. zapewniać jednakowe, lub zbliżone wyświetlanie wszystkich elementów we wspieranych przeglądarkach.	W	

37.	System w zakresie funkcji dostępnych dla pracowników administracji uczelni musi być dostępny z poziomu aplikacji możliwej do uruchomienia w środowisku Windows stosowanym powszechnie u Zamawiającego na stacjach roboczych.	W	
VII	Skalowalność i responsywność	W- Wymagane O - Opcjonalne	Tak/Nie
38.	System musi pozwalać na skalowanie następujących elementów środowiska: serwerów bazodanowych (klastry wydajnościowe i niezawodnościowe), serwerów aplikacyjnych, serwerów internetowych, liczby użytkowników nazwanych.	W	
39.	System musi zapewniać skalowalność dla wszystkich warstw architektury rozwiązania (skalowalność w poziomie i pionie) - nie może być wąskich gardeł stanowiących ograniczenie dla skalowania całego systemu.	W	
40.	Rozwiązanie musi umożliwiać różne konfiguracje instalacji, zachowując spójność jednego, niepowielanego systemu, np.: 1. system i baza danych na jednym serwerze, 2. system na osobnym serwerze, baza danych na osobnym serwerze, 3. wiele serwerów dostępowych.	W	
41.	System musi pracować na bazie danych, której silnik pozwala na: 1. utworzenie klastra,	W	

	2. pracuje jako usługa systemu, nie wymagająca zalogowania się użytkownika, startująca automatycznie wraz ze startem systemu operacyjnego, 3. stworzenie mirroringu online baz(y) danych.		
42.	Korzystanie przez użytkownika masowego (, studenta,) z systemu musi być możliwe za pomocą przeglądarki internetowej (Microsoft Edge 88 lub nowszej, Mozilla Firefox wersja 85 lub nowszej, Safari wersja 14 lub nowszej, Chrome wersja 88 lub nowszej, Opera wersja 73 lub nowszej) zainstalowanej na urządzeniu z odpowiednim systemem operacyjnym.	W	
VIII	Interoperacyjność i minimalne wymagania dla systemów teleinformatycznych	W- Wymagane O - Opcjonalne	Tak/Nie
43.	System musi być zgodny z wymaganiami dotyczącymi interoperacyjności, określonymi w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012, poz. 526 z późn. zm.)	W	

44.	System musi być interoperacyjny na poziomie technologicznym m.in. w zakresie: architektury (trójwarstwowa z warstwą prezentacyjną, aplikacyjną oraz danych) zgodnie z pryncypiami Architektury Zorientowanej Usługowo (SOA) lub REST API; bezpieczeństwa – system informatyczny musi być wdrożony w środowisku zapewniającym bezpieczeństwo dostępu, niezawodność i dostępność a także niezaprzeczalność, integralność i autentyczność danych; wykorzystanych standardów w protokołach komunikacyjnych i wymiany danych pomiędzy systemami.	W	
IX	Integracje i interfejsy integracyjne	W- Wymagane O - Opcjonalne	Tak/Nie
45.	System musi posiadać mechanizmy integracyjne z systemami obsługi Uczelni wykorzystywanymi przez Zamawiającego (Uczelnia wykorzystuje system Uczelnia 10)	W	
46.	Zastosowane w systemie formaty danych w zakresie publikowanych dokumentów cyfrowych muszą być zgodne z normami określonymi w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, oraz załącznikach do niego.	W	

47.	Formaty danych stosowanych przy wymianie informacji z innymi systemami muszą być zgodne z wymienionymi w załączniku nr 2 do Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych	W	
48.	System musi posiadać możliwość integracji danych i aplikacji z innymi systemami – relacyjnymi bazami danych (minimum obsługa ODBC/JDBC lub API).	W	
49.	Architektura systemu musi zapewniać otwartość na możliwość wymiany danych z innymi systemami za pomocą usług sieciowych (web services).	W	
X	System personalizacji kart	W- Wymagane O - Opcjonalne	Tak/Nie
50.	System personalizacji musi posiadać mechanizmy wymiany danych z systemami: kadrowym, dziekanatowym i rekrutacyjnym zgodnie z Ustawą z dnia 12 lutego 2010 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw (Dz. U. 210 nr 40 poz. 230 z późn. zm.)	W	
51.	System musi umożliwiać personalizację : • Elektronicznych Legitymacji Studenckich, • Elektronicznych Legitymacji Doktoranckich, • Elektronicznych Kart Pracowniczych. • Legitymacji Służbowych Nauczyciela Akademickiego	W	
52.	System musi umożliwiać przechowywanie danych osobowych oraz zdjęć w bazie danych systemu.	W	

53.	System musi posiadać możliwość odczytywania i zapisywania w bazie danych systemu pełnych (tj. unikatowych, UID) numerów fabrycznych (CSN) wydawanych kart odrębnie dla części stykowej i bezstykowej podczas personalizacji.	W	
54.	System musi umożliwiać wydawanie nowych kart oraz duplikatów	W	
55.	System musi zapewniać numerowanie (ELD) zgodnie z Rozporządzeniem Ministra Nauki i Szkolnictwa Wyższego z dnia 21 września 2018 r. w sprawie dyplomów doktorskich, dyplomów habilitacyjnych i legitymacji doktoranta (Dz.U. 2018 poz. 1837 z późn. zm.)	W	
56.	System musi umożliwiać generowanie raportów z wydań kart.	W	
57.	System musi zapewniać drukowania obydwu stron kart w jednym cyklu personalizacji w tym wydruku na kartach kodu kreskowego.	W	
58.	System musi umożliwiać inicjalizację i tworzenie struktury danych na kartach oraz (ELD) zgodnie z Rozporządzeniem Ministra Nauki i Szkolnictwa Wyższego z dnia 21 września 2018 r. w sprawie dyplomów doktorskich, dyplomów habilitacyjnych i legitymacji doktoranta (Dz.U. 2018 poz. 1837 z późn. zm.)	W	
59.	System musi umożliwiać inicjalizację i tworzenie struktury danych na kartach LSNA zgodnie z rozporządzeniem Ministra Nauki i Szkolnictwa Wyższego z dnia 13 marca 2020 r. w sprawie legitymacji służbowej nauczyciela akademickiego (Dz. U. 2020 poz. 689 z późn. zm.)	W	
60.	System musi umożliwiać zapis na kartach danych osobowych (ELD) zgodnie z rozporządzeniem Ministra Nauki i Szkolnictwa Wyższego z dnia 13 marca 2020 r. w sprawie legitymacji służbowej nauczyciela akademickiego (Dz. U. poz. 689 z późn. zm.), podpisanych certyfikatem własnym Punktu Personalizacyjnego lub certyfikatem kwalifikowanym operatora Punktu Personalizacyjnego wraz z zapisaniem użytego certyfikatu do pamięci karty.	W	
61.	System musi umożliwiać personalizację elektroniczną i graficzną kart w jednym przebiegu.	W	
62.	System musi umożliwiać obróbkę zdjęć zapisanych w postaci cyfrowej.	O	
63.	System musi umożliwiać definiowanie, co najmniej 20 grup obsługiwanych kart.	W	

64.	System musi umożliwiać definiowanie, co najmniej 20 różnych szablonów zadruku kart.	W	
65.	System musi posiadać możliwość drukowania potwierdzenia opłaty za wydanie karty.	O	
66.	System musi posiadać możliwość definiowania różnych taryf za wydanie karty i duplikatu.	W	
67.	System musi umożliwiać generowanie kluczy wzorcowych (mother keys), zapisywanych tylko i wyłącznie na karcie procesorowej.	W	
68.	Struktura danych na kartach (ELS, ELD, EKP, LSNA) powinna umożliwiać rozpoznanie wydawcy karty przy pomocy numeru identyfikacyjnego.	W	
69.	System musi umożliwiać: • rejestrację kart wzorcowych (z kluczami) w systemie, • wykonywania kopii kart z kluczami, • zmiany numerów PIN kart zawierających klucze, • odblokowywania numerów PIN kart z kluczami.	W	
70.	System musi umożliwiać generowanie • co najmniej 3 różnych kluczy wzorcowych dla części stykowej kart (ELS, ELD, EKP, LSNA), • co najmniej 16 różnych kluczy wzorcowych dla części bezstykowej standardu Mifare.	W	
71.	System powinien dla mechanizmu generowania kluczy wykorzystywać chwilowe wartości bufora klawiatury oraz pozycji myszki.	W	
72.	System musi posiadać mechanizm zabezpieczenia kart ELS, ELD, EKP, LSNA zarówno w części stykowej jak i bezstykowej. System powinien posiadać mechanizm dywersyfikacji kluczy w oparciu o wygenerowane klucze wzorcowe.	W	
73.	System powinien w trakcie instalacji oprogramowania wykorzystywać kartę z wygenerowanymi kluczami wzorcowymi jako narzędzie weryfikacji uprawnień do wykonania procesu instalacji oprogramowania.	W	
74.	System musi posiadać możliwość definiowania katalogu wejściowego zdjęć (przed obróbką).	W	

75.	System musi posiadać możliwość definiowania katalogu wyjściowego zdjęć (po obróbce).	O	
76.	System musi automatycznie uruchamiać aplikację do obróbki fotografii po zapisaniu zdjęć w katalogu wejściowym.	O	
77.	System musi posiadać obsługę następujących formatów plików graficznych: plik JPG (*.jpg, *.jpe, *.jpeg). PNG	W	
78.	System musi posiadać możliwość edycji następujących parametrów zdjęć: jasność, kontrast, nasycenie barw, rozmiar, skala, obrót, przesuwanie zdjęcia w pionie i poziomie.	O	
79.	System musi posiadać możliwość wykadrowania zdjęcia poprzez zaznaczenie obszaru kadrowania.	O	
80.	System musi posiadać możliwość podglądu i akceptacji wstępnie skadrowanego zdjęcia.	O	
81.	System musi posiadać możliwość cofnięcia i powtórzenia operacji kadrowania.	O	
82.	System musi umożliwiać automatyczne uruchamianie interfejsu umożliwiającego połączenie zdjęcia z danymi osobowymi po zaakceptowaniu kadru.	O	
83.	System musi umożliwiać automatyczne kierowanie obrobionych zdjęć do zdefiniowanego katalogu wyjściowego.	O	
84.	System musi posiadać możliwość wyszukiwania danych osobowych według filtra po następujących polach: Numer indeksu (albumu), Imię, Nazwisko, PESEL.	W	

85.	System musi umożliwiać przeglądanie listy wyszukanych osób wraz z możliwością edycji danych.	W	
86.	System musi umożliwiać włączenia automatycznego kierowania zadań wydruków kart do kolejki wydruków.	O	
87.	System musi posiadać możliwość definiowania trybu pracy programu – dostępne opcje konfiguracyjne co najmniej w zakresie: • personalizacja graficzna, • inicjalizacja elektryczna karty stykowej, • inicjalizacja elektryczna karty bezstykowej, • tworzenie logów zapisów dokonywanych na karty.	W	
88.	System musi umożliwiać sterowanie pracą drukarki do zadruku kart – dostępne opcje co najmniej w zakresie: • ładowanie karty do programatora, • wysuwanie karty, • zerowanie drukarki, • wydruk kontrolny, • test palety kolorów.	W	
89.	System musi umożliwiać konfiguracji programu, dostępne opcje konfiguracyjne co najmniej w zakresie: • wybór rodzaju drukarki z listy dostępnych, • wybór szablonu wydruku, • możliwość testowego wydruku szablonu.	W	



90.	System musi umożliwiać filtrowanie bazy danych po następujących polach co najmniej w zakresie: • numer indeksu (albumu), • imię, • nazwisko, • rodzaj szablonu, • wydział, •	W	
91.	System musi umożliwiać skierowanie do wydruku całej listy lub pojedynczych kart będących wynikiem filtrowania.	W	
92.	System musi posiadać możliwość podglądu statystyki bazy danych, dostępne pola co najmniej w zakresie: • liczba osób w bazie, • liczba osób, którym wydano kartę, • liczba osób, którym nie wydano karty, • liczba wydanych duplikatów, • liczba kart błędnie spersonalizowanych, • liczba zdjęć w bazie danych.	W	
93.	System musi posiadać możliwość podglądu statusu danych, dostępne statusy co najmniej w zakresie: • karta wydana, • karta ma zdjęcie, • karta jest repliką, • karta jest zawieszona, • karta jest duplikatem, • karta jest unieważniona, • wydano replikę/duplikat karty, • karta została zwrócona.	W	

94.	System musi umożliwiać wydruk duplikatu lub repliki karty.	W	
95.	System musi posiadać możliwość definiowania różnych kolejek wydruku i przypisywania im zadań według definiowanych przez użytkowników filtrów.	W	
96.	System musi posiadać możliwość integracji z AD w zakresie: • założenia konta AD, • edycji danych konta AD, • blokady konta AD. •	O	
97.	System musi posiadać możliwość integracji z Office 365.	W	
98.	System musi umożliwiać generowanie certyfikatów w procesie personalizacji i wgranie na ELS, ELD, LSNA w oparciu o lokalną domenę Uczelni.	W	
99.	Szczegółowy zakres integracji z systemami zewnętrznymi zostanie zdefiniowany na etapie analizy przedwdrożeniowej.	W	
100.	System musi umożliwiać zarządzania (nadanie, zamiana, reset) hasłami i PIN'ami do ELS, ELD, EKP, LSNA a także wysłanie ich na adres e-mail bądź wydruk na kopercie utajnionej.	O	
101.	System musi umożliwiać zarządzanie certyfikatami (wydanie, unieważnienie, unieważnienie czasowe, odnowienie) wgrywanymi na ELS, ELD, EKP, LSNA w procesie personalizacji.	O	
XI	Moduł MLegitymacji	W- Wymagane O - Opcjonalne	Tak/Nie
102.	System musi posiadać mechanizmy wymiany danych z systemem personalizacji zgodnie z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany	W	

	informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012, poz. 526 z późn. zm.)		
103.	System musi być zgodny z Rozporządzeniem Ministra Nauki i Szkolnictwa Wyższego z dnia 27.09.2018r w sprawie studiów (Dz. U. 2018 poz. 1861 z późn. zm.)	W	
104.	System musi być zintegrowany z centralnymi rejestrami (NASK) udostępniającymi dane legitymacji elektronicznej w aplikacji mObywatel.	W	
105.	System umożliwia pracownikowi dziekanatu utworzenie zlecenia wygenerowania mLegitymacji dla studenta bądź grupy studentów oraz anulowania mLegitymacji.	W	
106.	System musi umożliwić wygenerowanie oraz automatyczne wysłanie wiadomości e-mail do studenta z QRcode i kodem aktywacyjnym lub informacją o możliwości pobrania QRcode z witryny internetowej modułu mLegitymacja	W	
107.	System musi udostępniać witrynę internetową studentom, na której mogą wykonać następujące czynności : • zarejestrować zlecenie wygenerowania mLegitymacji • uzyskać i potwierdzić odbiór QRcode i kodu aktywacyjnego niezbędnego do użycia na urządzeniu mobilnym (mObywatel) • unieważnić mLegitymacje	W	
108.	System musi identyfikować następujące statusy mLegitymacji: • brak mLegitymacji – w przypadku gdy student ma aktywną elektroniczną legitymację studencką (ELS), nie została wygenerowana mLegitymacja ani nie istnieje aktywne zlecenie wygenerowania mLegitymacji • zlecona mLegitymacja – w przypadku gdy zostało zarejestrowane zlecenie wygenerowania mLegitymacji na witrynie internetowej	W	

	- błąd przetwarzania mLegitymacji – w przypadku gdy w trakcie przetwarzania wystąpił błąd - gotowa do odbioru mLegitymacja – w przypadku poprawnego przetworzenia zlecenia wygenerowania mLegitymacji (możliwość wysyłki wiadomości e-mail do studenta) - odebrana mLegitymacja – w przypadku poprawnego odebrania i aktywowania mLegitymacji na urządzeniu mobilnym - brak możliwości wygenerowania mLegitymacji – w przypadku gdy z jakiegoś powodu student nie może być posiadaczem mLegitymacji (np. nieaktywna legitymacja ELS) - anulowana mLegitymacja – w przypadku anulowania ważności mLegitymacji		
109.	System musi być zintegrowany z systemem personalizacji kart i udostępniać dane dot. mLegitymacji w części administracyjnej tego systemu.	W	
110.	System musi być zintegrowany z Windows AD Uczelni (np. ADFS) w zakresie identyfikacji i uwierzytelniania użytkowników.	W	
XII	Drukarka kart plastikowych	W- Wymagane O - Opcjonalne	Tak/Nie
111.	<u>Wymagania dla drukarki kart plastikowych</u> - Kompatybilna z zakupionym/posiadany/oferowanym oprogramowaniem do personalizacji kart. - Koder kart stykowych.	W	

	3. Koder kart bezstykowych. 4. Prędkość druku kolor jednostronnie: min 200 kart na godzinę. 5. Gwarancja na co najmniej 24 miesiące lub 10.000 kart. 6. Złącza USB i Ethernet. 7. W zestawie zapas taśmy na min 1.000 pełnych wydruków jednostronnych 8. Usługa instalacji i konfiguracji urządzenia do pracy z oprogramowaniem do personalizacji kart. Usługa może być zrealizowana zdalnie przy użyciu oprogramowania do udostępniania ekranu. Wykonanie testów wydruków.		
114.	Wymagania dla materiałów czyszczących 1. Kompatybilne z oferowaną drukarką. 2. Zapas zapewniający możliwość konserwacji drukarki przez okres 24 miesięcy przy prognozowanym wydruku 350 kart miesięcznie.	W	

....., dnia

.....
(podpis Wykonawcy)