

INFORMATOR DLA UCZELNI WYŻSZYCH

SYSTEM ELEKTRONICZNEJ LEGITYMACJI STUDENCKIEJ

1. Informacje ogólne.

1.1. Projekt graficzny – model legitymacji.



Wzór legitymacji



Wzór hologramu

1.2. Zalety wprowadzenia **Systemu Elektronicznej Legitymacji Studenckiej (SELS)**.

Każdy student rozpoczynający naukę otrzymuje poza indeksem także dokument potwierdzający bycie studentem – **legitymacje studencką**. Obecnie jest to papierowa książeczka zawierająca dane osobowe (tj. imię, nazwisko, adres zamieszkania) posiadacza legitymacji wraz z jego zdjęciem; określająca Uczelnię wyższą, jaka wystawiła dokument. Jej ważność przedłużana jest semestralnie poprzez postawienie pieczętki Uczelni w odpowiednim miejscu. Zaletą tego systemu jest m.in. łatwość wystawienia nowej legitymacji i jej duplikatu oraz łatwość przedłużania jej ważności. Posiada on jednak wiele wad, m.in.:

- małą odporność na uszkodzenia, zwłaszcza mechaniczne;
- podatność na różnego rodzaju fałszerstwa (nielegalne przedłużanie ważności dokumentu, zmianę danych posiadacza legitymacji);
- przyzwyczajenie ludzi do systemu legitymacji tradycyjnej.

Rozporządzenie MENiS z dnia 18 lipca 2005 r. w sprawie dokumentacji przebiegu studiów umożliwia, oprócz wydania studentowi legitymacji papierowej, **wydanie mu legitymacji w postaci karty elektronicznej**, co daje możliwość wprowadzenia **Systemu Elektronicznej Legitymacji Studenckiej (SELS)**.

SELS posiada kilka cech, które usprawnią działanie Uczelni wyższej, m.in.:

1. **SELS** jest **systemem wielofunkcyjnym** (**legitymacja elektroniczna** jest nie tylko dokumentem stwierdzającym, że jej posiadacz jest studentem Uczelni wyższej, lecz **przede wszystkim kartą elektroniczną, o wielorakich zastosowaniach** (np. jako karta biblioteczna). **Wielofunkcyjność** to także rozbudowany system informatyczny, na jakim oparty jest **SELS**, a którego zastosowanie w znacznym stopniu usprawni działalność Uczelni (dziekanatu, działu toku studiów, itd.)
2. **SELS** jest **bardziej odporny na różnego rodzaju fałszerstwa** (kartę elektroniczną znacznie trudniej podrobić).
3. **Legitymacja elektroniczna** jest też **bardziej odporna na przypadkowe zniszczenie czy też uszkodzenie danych**, zawartych w warstwie wizualnej, na skutek użytkowania dokumentu.

Wprowadzenie **Systemu Elektronicznej Legitymacji Studenckiej** przyniesie Uczelni wyższej:

- **rozwój systemu informatycznego** oraz **większą integrację** już istniejących podsystemów (dziekanatowego, bibliotecznego, obsługi stołówki, akademików);
- podniesie **bezpieczeństwo użytkowania legitymacji**;
- **ułatwi dostęp** studentom **do informacji** dla nich użytecznych;
- zwiększy **stopień bezpieczeństwa Uczelni**;
- zastosowanie **legitymacji elektronicznej** spowoduje **zastąpienie jedną kartą kilku różnych dokumentów** (m.in. karty bibliotecznej, karty stołkowej, itd.);
- **oszczędność czasu pracowników Uczelni** (np. student znaczną część informacji uzyskiwanych w dziekanacie będzie mógł sprawdzić w kioskach informacyjnych **SELS**).

1.3. Inne funkcje legitymacji elektronicznej.

Legitymacja elektroniczna oprócz funkcji podstawowej, może w zależności od potrzeb spełniać także inne funkcje, m.in.:

- karty bibliotecznej;
 - karty dostępowej;
 - karty upoważniającej do korzystania ze stołówki studenckiej;
 - karty upoważniającej do korzystania z parkingu uczelnianego;
 - biletu komunikacji miejskiej;
 - karty płatniczej (dokonywanie mikropłatności na terenie Uczelni).
-

1.4. Wykorzystanie elementów SELS w Systemie Elektronicznej Legitymacji Pracowniczej (SELP).

Wprowadzenie **Systemu Elektronicznej Legitymacji Studenckiej** spowoduje rozwój systemu informatycznego Uczelni w takim stopniu, że możliwe będzie wprowadzenie elektronicznej legitymacji pracowniczej w oparciu o infrastrukturę i doświadczenia zdobyte w trakcie wprowadzania **SELS**. Zasada działania **SELP** jest analogiczna do działania **SELS**. Legitymacja pracownicza może jednocześnie być dokumentem identyfikującym pracownika Uczelni wyższej jak i kartą dostępową do wydzielonych stref (np. miejsc pracy, pracowni dydaktycznych, itd.), kartą parkingową czy kartą biblioteczną. Oprócz wspólnych zastosowań z **SELS**, elektroniczna legitymacja pracownicza może służyć także jako karta monitorująca godziny pracy pracowników rozliczanych godzinowo. Wprowadzenie Systemu Elektronicznej Legitymacji Pracowniczej będzie procesem dużo łatwiejszym, ponieważ będzie oparte o istniejące już algorytmy powstałe podczas wdrażania **SELS** oraz o dobrze zintegrowany system informatyczny Uczelni.

2. Część szczegółowa.

Rozporządzenie MENiS z dnia 18 lipca 2005 r. w sprawie dokumentacji przebiegu studiów w załączniku nr 3 zawiera bardzo dokładny opis zarówno samej karty elektronicznej wykorzystanej jako **legitymacja elektroniczna** jak i opis danych zapisanych na karcie w warstwie wizualnej i elektronicznej. **Rozporządzenie jednoznacznie określa wzór legitymacji elektronicznej** (kolorystykę nadruków i tła legitymacji, wielkość i rodzaj czcionek użytych do wykonania napisów na niej umieszczonych, sposób zapisu danych w części elektronicznej karty itd.).

2.1. Dane przechowywane w legitymacji elektronicznej.

Zasadniczą funkcją **legitymacji studenckiej** jest **identyfikacja posiadacza** jako studenta Uczelni wyższej na jej terenie oraz poza nią. **Podstawowym elementem umożliwiającym identyfikację** są dane zawarte w postaci wizualnej. Są to: **zdjęcie** posiadacza legitymacji, **imię i nazwisko**, **numer PESEL**, **adres zamieszkania**, **data wydania legitymacji**, **numer albumu** (indeksu), **dane określające, jakim rodzajem dokumentu jest legitymacja** (napisy „LEGITYMACJA STUDENCKA” oraz „STUDENT CARD”), **dane określające Uczelnię**, która wydała legitymację (nazwa), **dane umożliwiające określenie ważności legitymacji (hologram)**. W przypadku zastosowania legitymacji jednocześnie jako karty bibliotecznej na rewersie karty umieszczony zostanie kod kreskowy identyczny, z tym jaki jest zastosowany w istniejących kartach bibliecznych. Informacje te, umieszczone na legitymacji, w dostatecznym stopniu spełniają rolę identyfikacyjną dokumentu i zawierają wszystkie dane z legitymacji tradycyjnej.

Część elektroniczna legitymacji przeznaczona jest do wykorzystania głównie na terenie Uczelni, gdzie będzie odpowiednia infrastruktura pozwalająca na odczyt informacji elektronicznych zawartych na karcie. Dane zapisywane w części elektronicznej w pliku **DF.SELS** oraz w plikach potomnych **EF.CERT** i **EF.ELS** zawierają następujące informacje:

- **plik EF.CERT dane dotyczące certyfikatu kwalifikowanego** określającego wystawiającego legitymacje;
- **plik EF.ELS dane dotyczące posiadacza legitymacji** (imię i nazwisko, numer PESEL, numer albumu studenta, nazwę Uczelni, datę ważności legitymacji, numer seryjny układu, oznaczenie rodzaju egzemplarza, datę ważności).

2.2. Cechy przyjętej technologii SELS.

Legitymacja studencka jest elektroniczną kartą procesorową z interfejsem stykowym określonym w normach ISO/IEC 7816-2 i ISO/IEC 7816-3 (legitymacja może zawierać również inne interfejsy, w tym interfejs bezstykowy w przypadku wykorzystania **elektronicznej legitymacji studenckiej** do kontroli dostępu do pomieszczeń, budynków, parkingów). Blankiet **legitymacji studenckiej** wykonany jest z materiału laminowanego o wymiarach 85,60 × 53,98 mm i właściwościach fizycznych zgodnych z wymaganiami dla kart identyfikacyjnych formatu ID-1 określonymi w normie ISO/IEC 7810, a jego właściwości i odporność muszą być potwierdzone badaniami przeprowadzonymi zgodnie z wieloczęściową normą ISO/IEC 10373.

2.3. Bezpieczeństwo SELS.

Zagadnienia bezpieczeństwa należy rozpatrywać z jednej strony w kontekście możliwych zagrożeń, a z drugiej kosztów możliwych do poniesienia przez uczelnie i studentów.

Falszerstwo legitymacji elektronicznej może wynikać z różnych motywacji:

- posiadanie legitymacji studenckiej jest związane z przywilejami finansowymi, takimi jak prawa do zniżek w środkach komunikacji i w wielu instytucjach kulturalnych;
- legitymacja umożliwia wstęp na imprezy zarezerwowane dla studentów;
- legitymacja zapewnia dostęp do bibliotek Uczelni, a także do wielu budynków;
- złamanie kodów zabezpieczających może być dla niektórych źródłem satysfakcji, a często wręcz fascynacji.

Odpowiedni poziom zabezpieczenia SELS zarówno w warstwie graficznej jak i w części elektronicznej powinien zniechęcić do działań wynikających z pobudek finansowych. Ewentualne zyski dla użytkownika karty nie mogą być wysokie. Jednak wiele będzie zależało od organizacji **SELS** w uczelniach, która powinna uniemożliwić dostęp do informacji poufnych osobom nieupoważnionym.

Elementy zabezpieczenia karty możemy podzielić na dwie grupy:

- a) **zabezpieczenia graficzne** (jednolity dla całego kraju projekt graficzny tła karty i samoprzylepny hologram potwierdzający termin ważności karty, numer kolejny karty, opcjonalnie kod kreskowy identyfikujący studenta w bazie bibliotecznej Uczelni wydającej kartę);

- b) **zabezpieczenia elektroniczne** - spójność informacji elektronicznej i graficznej (powtórzenie w układzie elektronicznym danych studenta i ważności karty), zabezpieczenie w postaci podpisu elektronicznego weryfikowanego kwalifikowanym certyfikatem w rozumieniu ustawy z dnia 18 września 2001 o podpisie elektronicznym.

Zagrożenia, ale zarazem możliwości ich neutralizowania, mogą pojawić się na każdym z etapów produkcji, wydawania, przedłużania terminu ważności i użytkowania **SELS**.

Etap	Źródło zagrożenia	Przeciwdziałania
Rozporządzenie MENiS	Ujawnienie szczegółów zabezpieczeń w tekście rozporządzenia	Poufność informacji o rodzajach zabezpieczeń graficznych i elektronicznych, brak precyzyjnych danych o stosowanych zabezpieczeniach graficznych i sposobie zapisu układu elektronicznego karty
Produkcja legitymacji i hologramów	1) Różnice w wyglądzie 2) Ujawnienie matrycy	1) Dopuszczenie do produkcji jedynie firm (produkcja chroniona) 2) MENiS dysponentem matrycy hologramu
Przesyłka kart i hologramów	Kradzież czystych dokumentów	Standardy przesyłek jak dla kart bankowych Numeracja kart przez producenta
Magazynowanie kart i hologramów	Kradzież czystych dokumentów	Procedury jak dla druków ścisłego zarachowania
Ochrona klucza prywatnego Uczelni	Możliwość skopiowania klucza	Wprowadzenie w Uczelni procedur wynikających z ustawy o podpisie elektronicznym, używanie jedynie nośników i procedur uniemożliwiających kopiowanie
Bezpieczeństwo bazy danych	Nieuprawniona modyfikacja bazy danych	Określenie uprawnień dostępu tylko dla niektórych pracowników, szkolenia pracowników
Przedłużanie ważności legitymacji	1) kradzież hologramów 2) modyfikacja danych osobowych	1) ściśle rozliczanie wydanych hologramów 2) w trakcie przedłużania możliwość modyfikacji jedynie terminu ważności SELS
Użytkowanie karty	Użycie fałszywych kart	Stała weryfikacja legitymacji przy ich użyciu w uczelniach

Ważnym zagadnieniem dotyczącym bezpieczeństwa SELS jest sposób postępowania w przypadku zgubienia czy kradzieży legitymacji. Strata legitymacji może spowodować nieautoryzowany dostęp do infrastruktury **SELS** przez osoby niepowołane, dlatego też podstawowym działaniem osoby, która straciła **ELS** jest zgłoszenie tego faktu celem unieważnienia dokumentu.

Algorytm unieważniania elektronicznej legitymacji studenckiej jest następujący:

- student, który utracił legitymację zgłasza się do administratora systemu;
- administrator na podstawie danych osobowych studenta potwierdzonych okazaniem dokumentu tożsamości (dowód osobisty, paszport itd.) wyszukuje dane studenta w systemie;
- po odnalezieniu danych administrator dokonuje unieważnienia utraconej legitymacji w całym systemie;
- po dokonaniu unieważnienia student udaje się do punktu wydawania legitymacji celem otrzymania nowej karty.

2.4. Trwałość karty elektronicznej.

Bardzo ważnym aspektem wdrażania **SELS** jest trwałość nośnika, czyli karty elektronicznej.

Tradycyjna legitymacja wykonana w postaci papierowej książeczki **jest dokumentem wrażliwym na uszkodzenia** mechaniczne (ścieranie pod wpływem użytkowania, zadrapania, przypadkowe zalanie cieczą) prowadzące do zniekształcenia danych w niej zawartych.

Elektroniczna Legitymacja Studencka jest kartą elektroniczną wykonaną z tworzywa sztucznego, **trwałą i odporną na ścieranie**. Dobrze wykonana karta (przez firmę posiadającą certyfikat Arsenal Institut z Wiednia lub innej autoryzowanej jednostki certyfikującej) jest odporna na:

- zalanie lub też zamoczenie różnymi rodzajami płynów (m.in. bada się wpływ różnych kwasów spożywczych na kartę);
- promieniowanie elektromagnetyczne emitowane przez różne popularne urządzenia elektroniczne i elektryczne np. telefon komórkowy, monitor komputera;
- inne czynniki, wynikające z normalnego użytkowania karty (m.in. czynniki mechaniczne i termiczne).

Karta elektroniczna jest dokumentem **trwalszym i bardziej odpornym** na różnego rodzaju szkodliwe czynniki wynikające z normalnego użytkowania legitymacji, niż dotychczas używana legitymacja papierowa. Trwałość układu elektronicznego zależy od technologii, w jakiej został wykonany. Przeciętna **karta stykowa posiada minimum dziesięcioletnią trwałość przechowywania danych** i możliwość wykonania ok. 100000 cykli zapisu lub odczytu danych.

Podsumowując, trwałość karty zapewnia poprawne funkcjonowanie legitymacji elektronicznej przez okres pięcio- lub sześcioletnich studiów.

2.5. Infrastruktura potrzebna do wdrożenia oraz użytkowania **SELS**.

SELS jest **systemem informatycznym** w znacznym stopniu **integrującym różne systemy informatyczne** działające w ramach Uczelni wyższej tj. system obsługi dziekanatów, system biblioteczny oraz inne systemy funkcjonujące na danej Uczelni. Z punktu widzenia informatycznego **SELS jest systemem bazodanowym o układzie wieloaplikacyjnym**. W skład takiego systemu wchodzi wiele aplikacji, baz danych, specjalistycznych urządzeń dających zintegrowany system informatyczny pozwalający na wykorzystanie zalet **legitymacji elektronicznej** (karty elektronicznej).

W skład oprogramowania wykorzystywanego przez **SELS** wchodzi:

- **baza danych**;
 - **systemy operacyjne**, na których oparte są **serwery SELS**;
 - **oprogramowanie dla stacji roboczych** wykorzystywanych w **SELS**;
 - **oprogramowanie specjalistyczne** przeznaczone do obsługi i zarządzania systemem elektronicznej legitymacji studenckiej.
-

Rodzaje zastosowanych baz danych i systemów operacyjnych obsługujących serwery i stacje robocze **SELS** są polecane przez firmy wdrażające systemy kart elektronicznych wraz z oprogramowaniem specjalistycznym (moduły administracyjne, personalizacyjne, kontroli dostępu i inne w zależności od projektu wykorzystania karty elektronicznej).

Od strony sprzętowej w skład **SELS** wchodzi:

- **serwery baz danych;**
- **komputery** służące jako **stacje personalizacyjne, administracyjne** oraz obsługujące inne funkcje **SELS**;
- **drukarki do zadruku kart** wyposażone w **kodery kart stykowych i bezstykowych** (tylko w opcji personalizacji kart dokonywanej na terenie Uczelni);
- **skanery** lub też **aparaty cyfrowe** służące do wprowadzania zdjęć posiadaczy legitymacji do modułu personalizacyjnego;
- **czytniki kodów kreskowych;**
- **drukarki komputerowe** do wydruku potwierdzeń odbioru legitymacji, zestawień, raportów i innych dokumentów używanych w obsłudze **SELS**;
- **terminale** umożliwiające posiadaczom elektronicznej legitymacji studenckiej **dostęp do informacji SELS** (np. informacji dziekanatowych lub bibliotecznych);
- opcjonalnie **czytniki kart bezstykowych** standardu MIFARE Standard (**kontrola dostępu**);
- opcjonalnie **układy zamków elektromechanicznych** z zasilaniem (**kontrola dostępu**).

Część wyżej wymienionego sprzętu i oprogramowania znajduje się w systemie informatycznym Uczelni i nadaje się do wykorzystania w **SELS** (głównie serwery, stacje robocze, systemy operacyjne), część natomiast należy zakupić.

2.6. Walidacja ważności ELS (przedłużanie ważności ELS).

Niezmiernie **ważnym aspektem** związanym nie tyle z **Systemem Elektronicznej Legitymacji Studenckiej** lecz z samą **legitymacją studencką** w postaci karty elektronicznej, jest **walidacja** (potwierdzenie terminu) jej ważności. Jest to kwestia niezmiernie ważna nie tylko dla studenta, ale także dla całego systemu **SELS** i jego bezpieczeństwa. **Sprawdzania ważności legitymacji elektronicznej** można dokonać w **dwóch warstwach**:

- **warstwie wizualnej**, głównie poza Uczelnią – przy pomocy naklejonego na legitymację hologramu z naniesioną datą ważności;
- **warstwie elektronicznej**, głównie na terenie Uczelni (infrastruktura **SELS**) – poprzez sprawdzenie zakodowanej w części elektronicznej karty daty ważności legitymacji.

Przedłużanie ważności legitymacji następuje przez naklejenie na rewersie legitymacji **samoprzylepnego hologramu** zawierającego datę ważności legitymacji. Konstrukcja samego hologramu uniemożliwia jego odklejenie bez uszkodzenia. Po naklejeniu hologramu data ważności kodowana jest w pamięci legitymacji przy pomocy kodera. Proces ten powinien odbywać się w dziekanacie lub punkcie wydawania legitymacji, w zależności od liczby obsługiwanych studentów.

2.7.Sposób personalizacji, wydawania ELS.

Wydawanie ELS jest procesem złożonym z uwagi na dużą ilość danych zawartych w samej legitymacji, które muszą być spójne w dwóch warstwach – wizualnej i elektronicznej. Część elementów umieszczonych na karcie jest wspólna dla wszystkich legitymacji wydawanych na danej uczelni wyższej i są one nanoszone i chronione zewnętrzną folią laminacyjną w procesie produkcji karty. Dane indywidualne studenta nanoszone są w procesie personalizacji legitymacji.

W procesie produkcji nanoszone są na kartę metodą poddruku offsetowego następujące elementy:

- tło z elementami grafiki rastrowej;
- zabezpieczające elementy wykonane techniką giloszową;
- napis „LEGITYMACJA STUDENCKA” umieszczony na białym pasku o szerokości 1mm przebiegającym poziomo w odległości 1,7 mm od dolnej krawędzi karty;
- godło państwowe i napis „Rzeczpospolita Polska”;
- napisy: „LEGITYMACJA STUDENCKA”, „STUDENT CARD”, „Wydana:”, „Nr albumu:”, „PESEL”, „Adres:”, „Legitymacja ważna do:”, „Poświadcza uprawnienia do korzystania z ulgowych przejazdów środkami publicznego transportu zbiorowego kolejowego i autobusowego, a także środkami komunikacji miejskiej, na podstawie odrębnych przepisów”;
- biały obszar przeznaczony na zdjęcie posiadacza legitymacji;
- 12 pól oznaczonych kolejno cyframi od 1 do 12;
- obszar biały przeznaczony na naniesienie kodu kreskowego.

W procesie personalizacji legitymacji studenckiej nanoszone są za pomocą drukarki termosublimacyjnej następujące, chronione warstwą zabezpieczającą, dane:

- kolorowe zdjęcie posiadacza legitymacji;
- nazwa Uczelni w dwóch lub trzech wierszach, do 30 znaków w wierszu;
- imię do 24 znaków oraz nazwisko w dwóch wierszach, do 28 znaków każdy;
- adres, w dwóch wierszach do 40 znaków każdy;
- data wydania;
- nr albumu;
- numer PESEL (dla obcokrajowców data urodzenia w formacie rrrmdd00000);
- kod kreskowy (opcjonalnie).

Proces personalizacji legitymacji może być przeprowadzany na dwa sposoby, na zewnątrz bądź też wewnątrz Uczelni. Personalizacja kart powinna odbywać się według zasad obowiązujących dla druków ścisłego zarachowania. Obszar układu elektronicznego nie może być personalizowany z żadnej strony karty.

Do wad personalizacji dokonywanej przez firmy zewnętrzne możemy zaliczyć:

- dłuższy czas oczekiwania na wydanie nowej karty czy też duplikatu;
 - personalizacja seriami po kilkadziesiąt sztuk;
 - mniejsze bezpieczeństwo danych osobowych;
 - większa możliwość popełnienia pomyłek;
 - przygotowywanie danych do personalizacji dla każdej serii oddzielnie.
-

Zaletami tego sposobu personalizacji są:

- **odpowiedzialność za techniczne błędy w personalizacji ponosi firma zewnętrzna;**
- **firma może dokonywać dystrybucji tych kart** (np. przesyłać je pocztą do studenta);
- **stałe koszty jednostkowe personalizacji pojedynczej legitymacji studenckiej.**

Metoda personalizacji **wewnątrz Uczelni** przynosi następujące **korzyści**:

- **czas oczekiwania** na wydanie legitymacji bądź jej duplikatu jest **praktycznie zerowy** (trwa tyle, ile naniesienie danych na kartę);
- **możliwość wydania do 200 legitymacji dziennie** (na jednej drukarce);
- brak potrzeby przygotowywania danych potrzebnych do personalizacji, **karty wydawane są „od ręki”**;
- **ułatwiony dostęp** do innych **systemów informatycznych Uczelni**, a co za tym idzie znaczna **łatwość pobrania danych do zapisu w części elektronicznej karty**;
- **brak zagrożeń** związanych z **bezpieczeństwem przesyłania danych** do firmy zewnętrznej.

Wady tego rozwiązania to:

- **brak opłacalności ekonomicznej przy małej ilości kart wydawanych rocznie** (komercyjne firmy wdrażające systemy kart elektronicznych przyjmują próg opłacalności finansowej uruchomienia punktu personalizacyjnego na Uczelni na poziomie 2500 kart wydawanych rocznie);
- **koszty zatrudnienia osób** dokonujących personalizacji;
- **koszty wyposażenia pomieszczeń**, zakupu urządzeń do personalizacji.

2.8. Analiza kosztów.

Poniższe dane są jedynie szacunkowe i mogą się zmienić w zależności od wielkości zamówienia i rozwoju technologii.

Lp.	Opis elementu	Cena netto dla 5000 kart	Cena netto dla 10000 kart
1	Karta stykowa PCW + tło dwustronne 4/1 (poddruk pod folią laminującą)	12zł	9,8zł
2	Personalizacja (zdjęcie + napisy) / 4 kolory (metodą termosublimacji)	4 zł	2,8zł
3	Hologram samoprzylepny (bez matrycy)	0,4 zł	0,2zł
4	Urządzenie do jednostronnej personalizacji karty metodą termosublimacji + koder pamięci układu stykowego	13000 – 15000 zł	
5	Urządzenie do dwustronnej personalizacji karty metodą termosublimacji + koder pamięci układu stykowego	15000 – 25000zł	

Korzystniejsze ekonomicznie są rozwiązania, w których hologram z datą ważności jest dostarczany do Uczelni. Po naklejeniu w dziekanacie hologramu na karcie należy użyć kodera, który modyfikuje informację w pamięci układu stykowego karty. Umieszczanie kodu kreskowego (używanego w systemie bibliotecznym) na rewersie karty zwiększy koszt drukarki personalizującej karty. Jest to jednak dla Uczelni wydatek jednorazowy.

W fazie pilotażowej projektu powinno się ocenić, ile urzędzeń do personalizacji koniecznych jest do sprawnego semestralnego przedłużania legitymacji. Można szacować, że jedno urządzenie + koder pamięci powinny obsługiwać nie więcej niż 5000 studentów, aby czas przedłużenia semestralnego legitymacji nie przekroczył 2 tygodni.

2.9. Potencjalne utrudnienia i zagrożenia jakich należy spodziewać podczas wprowadzania SELS

Podczas wdrażania każdego projektu **SELS** potencjalne zagrożenia czy utrudnienia możemy podzielić na dwie kategorie: na **zagrożenia techniczne** oraz zagrożenia **spowodowane czynnikiem ludzkim**. Pierwszy rodzaj wynika m.in. z użytej technologii, zastosowanego oprogramowania, sprzętu, natomiast drugi ze sposobu przyjmowania nowości technicznych przez ludzi lub przyzwyczajenia do sprawdzonych metod funkcjonowania.

Utrudnienia techniczne to m.in.:

- **utrudnienia związane z systemem informatycznym** Uczelni, jego infrastrukturą oraz oprogramowaniem. **SELS** jest systemem wielofunkcyjnym i wielomodułowym opartym na integracji w jedną sieć informatyczną kilku różnych systemów informatycznych funkcjonujących na Uczelni wyższej. **Oznacza to wysoki stopień niepewności działania takiego systemu.**
- **brak kompatybilności** pomiędzy systemami informatycznymi Uczelni a **SELS**, spowodowany wykorzystywaniem przez uczelnie różnych rozwiązań systemów informatycznych, a co się z tym wiąże, utrudnioną wymianą informacji pomiędzy systemami.

Bardzo istotną sprawą podczas wprowadzania **SELS** będzie **odbiór przez społeczność akademicką tego systemu**. Część ludzi przyjmie **legitymację elektroniczną** jako ułatwienie w pracy czy też studiowaniu, ale część społeczności akademickiej Uczelni okaże nieprzychylnie nastawienie dla wprowadzania **SELS**, które może wynikać z różnych przyczyn, m.in.:

- **niechęci** do nowości technicznych;
- **przyzwyczajenia do starego systemu** i niechęci porzucania sprawdzonych procedur i algorytmów działania na rzecz nowych, jeszcze niesprawdzonych;
- **obawy** przed nieznanym;
- niechęci spowodowanej wadliwym działaniem systemu.

Zagrożeń i utrudnień, na jakie narażone jest wprowadzanie **SELS**, jest dużo. Każdy złożony projekt informatyczny posiada ich wiele, jednak zalety i korzyści z niego płynące rekompensują je całkowicie.

2.10 . Specyfikacja istotnych warunków zamówienia elementów infrastruktury sprzętowej i programowej (w tym kart) SELS.

Rozporządzenie MENiS z dnia 18 lipca 2005 r. w sprawie dokumentacji przebiegu studiów (załącznik nr 3) podaje bardzo dokładną specyfikację karty elektronicznej, jaka ma stanowić **legitymację elektroniczną**. Dlatego zamówienia dotyczące elementów **SELS** będą dotyczyły elementów infrastruktury sprzętowej **SELS** jak i oprogramowania użytego w systemie legitymacji elektronicznej. Rodzaj, ilość, koszt czy producent sprzętu i oprogramowania **SELS** zależy w głównej mierze od:

- stanu systemów informatycznych Uczelni w momencie wdrażania **SELS**;
- rodzaju dodatkowych funkcji, jakie będzie spełniać legitymacja elektroniczna na danej Uczelni;
- wielkości Uczelni.

Ogólnie rzecz ujmując specyfikacja zamówienia **SELS** powinna zawierać:

- opis funkcji, jakie ma spełniać **SELS**;
- cechy i sposób połączenia istniejących systemów informatycznych z **Systemem Elektronicznej Legitymacji Elektronicznej**;
- opis struktury logicznej **SELS**:
 - sposób i rodzaj wyposażenia punktów wydawania legitymacji (punkt personalizacji wewnątrz Uczelni czy tylko miejsce wydawania legitymacji spersonalizowanych przez firmę zewnętrzną);
 - ilość i rozmieszczenie punktów dostępu do informacji zawartych w **SELS** (kioski informacyjne);
 - rozmieszczenie i rodzaj czytników kart elektronicznych (kontrola dostępu);
- opis struktury informatycznej **SELS**:
 - procedury obiegu informacji w systemie;
 - procedury bezpieczeństwa;
 - algorytmy wydawania i przedłużania ważności legitymacji;
 - rodzaj informacji udostępnionych studentom w kioskach informacyjnych.

Proces wdrożenia **Systemu Elektronicznej Legitymacji Studenckiej** można podzielić na **dwie** kluczowe fazy: **projektowanie i wdrożenie**.

W fazie projektowania należy:

- wykonać analizę biznesową projektu wdrażania **SELS**;
 - określić, kto ma kierować projektem (administracja czy IT);
 - określić, kto ma być zaangażowany w projekt;
 - przygotować ogólną strategię wdrożeniową, na którą składa się:
 - analiza istniejących systemów informatycznych na Uczelni;
 - analiza obecnych i przyszłych potrzeb systemu karty studenckiej;
 - analiza rozwiązań istniejących w innych uczelniach;
 - analiza najnowszych rozwiązań;
 - określenie wariantów i opcji;
-

- **określić menedżera projektu;**
- **utworzyć grupę wdrożeniową** (przedstawiciele wszystkich działów i grup, na których funkcjonowanie może mieć wpływ system kartowy, reprezentacja studentów, itd.);
- **ustalić rolę oraz regulamin działania grupy wdrożeniowej;** działania grupy powinny obejmować cały projekt (wszystkie jego aspekty);
- **opracować plan wdrożenia systemu:**
 - określenie zakresu **SELS**;
 - określenie sposobu personalizacji legitymacji;
 - ustalenie celów, które należy osiągnąć;
 - określenie, jakie aplikacje i funkcje zostaną wdrożone (np. korzystanie z biblioteki, kontrola dostępu, kioski informacyjne, itp.)
 - ustalenie harmonogramu wdrożenia;
 - opracowanie procedur wydawania legitymacji a także procedur bezpieczeństwa, jakie zostaną zastosowane w **SELS**.
- **zaprojektować i wyprodukować materiały promocyjne** (książeczka instruktażowa, przewodnik po systemie, informacje w materiałach dla studentów);
- **dokonać oceny stanu infrastruktury uczelnianej,** określić niezbędne modyfikacje, nie tylko sieci informatycznej, ale także elektrycznej, logicznej oraz uczelnianego systemu bezpieczeństwa w celu ewentualnej modyfikacji pod kątem wdrażania **SELS**.
- **określić sposób wdrażania SELS** (całościowo czy etapowo).

Faza wdrożeniowa to złożony proces wprowadzania **SELS** w życie:

- **uruchomienie infrastruktury sprzętowo – programowej SELS;**
- **integracja SELS** z infrastrukturą Uczelni;
- **stworzenie infrastruktury logicznej systemu;**
- **szkolenie obsługi systemu;**
- **zbieranie danych** potrzebnych do personalizacji legitymacji (zdjęcia studentów, dane osobowe itd.);
- **wprowadzenie regulaminu** wydawania i użytkowania legitymacji;
- **wprowadzanie procedur bezpieczeństwa i systemów zabezpieczeń SELS;**
- **wychwytywanie błędów** we wdrażanym systemie.

Podsumowując, wdrażanie **SELS** polega na:

- ustaleniu wymagań i zakresu systemu;
 - przygotowaniu dobrego planu;
 - zapewnieniu sobie całkowitej kontroli nad systemem;
 - zapewnieniu sobie współpracy z dobrym partnerem – integratorem systemu;
 - zorganizowaniu efektywnego zespołu zarządzania.
-