Załącznik nr 8 do SIWZ, załącznik 6 do umowy, Załącznik 2 do OPZ – Wymagania funkcjonalne SYSTEMU Personalizacji ELP i PKI

Wymagania funkcjonalne SYSTEMU Personalizacji ELP oraz PKI

1. System Personalizacji ELP

L.p.	OPIS FUNKCJONALNOŚCI
1	Zamawiający wymaga wdrożenia systemu do personalizacji kart procesorowych ELP wydawanych pracownikom administracyjnym,
2	System personalizacji musi posiadać mechanizmy wymiany danych z systemem ERP zgodnie z Rozporządzeniem Rady Ministrów z dnia 11.10.2005 roku w sprawie minimalnych wymagań dla rejestrów publicznych i wymiany informacji w formie elektronicznej,
3	System musi umożliwiać personalizację Elektronicznych Legitymacji Pracowniczych (ELP),
4	System musi umożliwiać przechowywanie danych osobowych oraz zdjęć w bazie danych systemu,
5	System musi posiadać możliwość odczytywania i zapisywania w bazie danych systemu numerów fabrycznych (CSN) wydawanych kart odrębnie dla części stykowej i bezstykowej podczas personalizacji,
6	System musi umożliwiać wydawanie nowych kart oraz duplikatów,
7	System musi umożliwiać generowanie raportów z wydań kart,
8	System musi zapewniać drukowanie obydwu stron kart w jednym cyklu personalizacji w tym wydruku na kartach kodu kreskowego.
9	System musi umożliwiać inicjalizację i tworzenie struktury danych na kartach ELP,
10	System musi umożliwiać zapis na kartach danych osobowych ELP podpisanych certyfikatem własnym (niekwalifikowanym) Punktu Personalizacyjnego lub certyfikatem kwalifikowanym operatora Punktu Personalizacyjnego wraz z zapisaniem użytego certyfikatu do pamięci karty,
11	System musi umożliwiać personalizację elektroniczną i graficzną kart w jednym przebiegu.
12	System musi umożliwiać obróbkę zdjęć zapisanych w postaci cyfrowej.
13	System musi umożliwiać definiowanie, co najmniej 20 grup obsługiwanych kart.
14	System musi umożliwiać definiowanie, co najmniej 20 różnych szablonów zadruku kart.
15	System musi posiadać możliwość drukowania potwierdzenia opłaty za wydanie karty.
16	System musi posiadać możliwość definiowania różnych taryf za wydanie karty i duplikatu.
17	System musi umożliwiać generowanie kluczy wzorcowych (mother keys), zapisywanych tylko i wyłącznie na karcie procesorowej.
18	Struktura danych na kartach ELP powinna umożliwiać rozpoznanie wydawcy karty przy pomocy numeru identyfikacyjnego.
19	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
20	System musi umożliwiać generowanie co najmniej 3 różnych kluczy wzorcowych dla części stykowej kart ELP
21	System musi umożliwiać generowanie co najmniej 16 różnych kluczy wzorcowych dla części bezstykowej standardu Mifare
22	System powinien wykorzystywać dla mechanizmu generowania kluczy chwilowe wartości bufora klawiatury oraz pozycji myszki.
23	System musi posiadać mechanizm zabezpieczenia kart ELP zarówno w części stykowej jak i bezstykowej. System powinien posiadać mechanizm dywersyfikacji kluczy w oparciu o wygenerowane klucze wzorcowe.
24	System powinien w trakcie instalacji oprogramowania wykorzystywać kartę z wygenerowanymi kluczami wzorcowymi jako narzędzie weryfikacji uprawnień do wykonania procesu instalacji oprogramowania.
25	System musi posiadać możliwość definiowania katalogu wejściowego zdjęć (przed obróbką).

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego i wdrażany w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020, zgodnie z umową o dofinansowanie nr POWR.03.05.00-00-Z068/18

26	System musi posiadać możliwość definiowania katalogu wyjściowego zdjęć (po obróbce).
27	System musi posiadać umożliwiać obsługę następujących formatów plików graficznych: mapa bitowa (*.bmp), plik JPG (*.jpg, *.jpe, *.jpeg).
28	System musi posiadać możliwość edycji następujących parametrów zdjęć: jasność, kontrast, nasycenie barw, rozmiar, skala, obrót, przesuwanie zdjęcia w pionie i poziomie.
29	System musi posiadać możliwość wykadrowania zdjęcia poprzez zaznaczenie obszaru kadrowania.
30	System musi posiadać możliwość podglądu i akceptacji wstępnie skadrowanego zdjęcia.
31	System musi posiadać możliwość cofnięcia i powtórzenia operacji kadrowania.
32	System musi umożliwiać automatyczne uruchamianie interfejsu umożliwiającego połączenie zdjęcia z danymi osobowymi po zaakceptowaniu kadru.
33	System musi umożliwiać automatyczne kierowanie obrobionych zdjęć do zdefiniowanego katalogu wyjściowego.
34	System musi posiadać możliwość zapisania w bazie danych nowego zdjęcia.
35	System musi posiadać możliwość podmiany zdjęcia wcześniej zapisanego w bazie danych.
36	System musi posiadać możliwość wyszukiwania danych osobowych według filtru po następujących polach: Numer indeksu (albumu), Imię, Nazwisko, PESEL.
37	System musi umożliwić automatyczne, okresowe (przy zdefiniowanej częstotliwości) pobieranie danych osobowych (synchronizację) niezbędnych w procesie personalizacji.
38	System musi umożliwiać ręczne wprowadzanie danych osobowych (np. kart gości, parkingowych, itp.).
39	System musi umożliwiać przeglądanie listy wyszukanych osób.
40	System musi umożliwiać włączenie automatycznego kierowania zadań wydruków kart do kolejki wydruków.
41	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
42	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
43	System musi umożliwiać konfigurację programu, dostępne opcje konfiguracyjne co najmniej w następującym zakresie: wybór rodzaju drukarki z listy dostępnych, wybór szablonu wydruku, możliwość testowego wydruku szablonu
44	System musi umożliwiać filtrowanie bazy danych po następujących polach co najmniej w zakresie: numer teczki pracownika, imię, nazwisko, rodzaj szablonu, obecność zdjęcia przypisanego do rekordu,
45	System musi umożliwiać skierowanie do wydruku całej listy lub pojedynczych kart będących wynikiem filtrowania
46	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
47	System musi posiadać możliwość podglądu statusu danych, dostępne statusy co najmniej w zakresie: karta wydana, karta ma zdjęcie, karta jest duplikatem, karta jest zawieszona, karta jest unieważniona, wydano duplikat karty, karta została zwrócona.
48	System musi umożliwiać wydruk duplikatu karty.
49	System musi posiadać możliwość definiowania różnych kolejek wydruku i przypisywania im zadań według definiowanych przez użytkowników filtrów.
50	System musi posiadać możliwość integracji z AD w zakresie uwierzytelnienia do systemu wybranych przez administratora użytkowników,
51	System musi posiadać możliwość integracji z Office 365.
52	System musi umożliwiać integrację z systemem Kontroli Dostępu: ICT Protege GX posiadanym przez Zamawiającego, wywołując udostępnione mechanizmy integracji w przypadku: Wydania nowej kart, Wydania duplikatu kart, Unieważnienia karty
53	System musi umożliwiać integrację z autorskim systemem Kontroli Dostępu posiadanym przez Zamawiającego, poprzez przygotowanie widoku bazodanowego zawierającego listę osób/kart aktywnych i nieaktywnych, wraz z numerem MiFare karty

54	System musi być zintegrowany z systemem ERP umożliwiając z poziomu formularza systemu ERP zlecenie wydruku karty, duplikatu
55	System personalizacji musi przekazywać dane podstawowe o karcie pracownika zwrotnie do systemu ERP,
56	System personalizacji musi umożliwiać rozbudowę o personalizację Elektronicznych Legitymacji Studenckich (ELS), Elektronicznych Legitymacji Doktoranckich (ELD) oraz Elektronicznych Legitymacji Nauczyciela Akademickiego (ELNA) – rozbudowa ta nie jest przedmiotem tego postępowania,
57	System personalizacji musi umożliwiać w przyszłości rozbudowę o integrację z systemem PEKA https://www.peka.poznan.pl – integracja i wdrożenie nie jest przedmiotem tego postępowania.
58	Szczegółowy zakres integracji zostanie zdefiniowany na etapie analizy przedwdrożeniowej.

2. System PKI (Infrastruktura Klucza Publicznego)

L.p.	OPIS FUNKCJONALNOŚCI
1	Wdrożenie systemu personalizacji kart musi obejmować wdrożenie uczelnianego centrum certyfikacji – PKI obejmującego zaufaniem pracowników Uczelni.
2	Certyfikaty muszą zapewnić możliwość ich wykorzystania podczas: Uwierzytelnienia wybranych użytkowników do systemu operacyjnego stacji roboczej / komputera, autoryzacji kluczowych czynności użytkowników w systemie ERP; z możliwością wyłączenia tego mechanizmu dla danego użytkownika przez administratora systemu ERP, podpisywania poczty elektronicznej lub innych dokumentów, szyfrowania poczty elektronicznej lub innych dokumentów.
3	Proces uwierzytelnienia realizowany w systemie musi wykorzystywać układ stykowy kart procesorowych ELP,
4	Zamawiający wymaga wystawiania i wgrywania certyfikatów na nowe, dostarczone przez Wykonawcę karty pracowników Uczelni.
5	Usługi katalogowe muszą umożliwiać przechowywanie klucza publicznego, a pozycje katalogu opisujące użytkowników muszą zawierać atrybut umożliwiający rozróżnienie grupy użytkowników (co najmniej podział: pracownik administracji/nauczyciel akademicki/student/doktorant/inny)
6	Oprogramowanie PKI musi umożliwić definiowanie celów dla wystawianych certyfikatów (np. uwierzytelnianie, podpis, szyfrowanie),
7	Czynności administracyjne dotyczące zarządzania certyfikatami muszą umożliwiać: czasowe zablokowanie certyfikatu, odblokowanie certyfikatu czasowo zablokowanego, całkowite unieważnienie certyfikatu, odnowienie certyfikatu.
8	Oprogramowanie PKI musi umożliwiać unieważnianie certyfikatów oraz musi publikować listy CRL (listy certyfikatów unieważnionych), a także wspierać protokół OCSP (Online Certificate Status Protocol),
9	Oprogramowanie PKI musi umożliwiać administratorowi indywidualne utworzenie certyfikatów dla wybranych użytkowników, na wypadek utraty/unieważnienia aktualnego certyfikatu,
10	Oprogramowanie PKI musi umożliwić ustalenie odrębnego okresu ważności generowanych certyfikatów dla zdefiniowanych grup użytkowników,
11	Oprogramowanie PKI musi umożliwiać przechowywanie i wygenerowanie dla użytkowników kluczy prywatnych i certyfikatów w plikach w formacie PKCS#12, w którym do szyfrowania zastosowano PIN administracyjny, wygenerowany w czasie inicjalizacji karty kryptograficznej,
12	Oprogramowanie PKI musi przygotowywać ELP do obsługi PKI w procesie personalizacji blankietu, przez co Zamawiający rozumie m.in. wykonanie następujących czynności: wygenerowanie żądania certyfikatu dla tego konta, wygenerowanie PIN-ów, dystrybucja certyfikatów. W trakcie procesu personalizacji ELP musi zostać wygenerowany indywidualny numer PIN użytkownika dla każdej karty. PIN do karty musi być co najmniej 6 znakowy. System musi zapewniać możliwość wydruku numeru PIN karty w poufny sposób na kopertach utajonych.
13	Oprogramowanie PKI w trakcie przygotowania ELP do obsługi PKI musi wygenerować także 8 cyfrowy PIN administracyjny.
14	Oprogramowanie PKI musi przygotować ELP do obsługi PKI w procesie przedłużania ważności w Systemie.
15	Oprogramowanie PKI musi umożliwiać wydanie dla każdego użytkownika co najmniej jednego zestawu kluczy z certyfikatami. Liczba wydawanych certyfikatów powinna być konfigurowalna w obrębie grup.
16	Oprogramowanie PKI musi umożliwiać generowanie pary kluczy RSA (1024 bit oraz 2048 bit) przez karty ELP lub system operacyjny.
17	Oprogramowanie musi umożliwiać wybór szablonu do utworzenia certyfikatu. Szablon musi mieć możliwość definiowania listy atrybutów umieszczanych w certyfikacie oraz przeznaczenia klucza.
18	Dane zapisywane na karcie w formacie PKCS#12 muszą być archiwizowane w bazie Systemu Personalizacji Kart używanym przez Zamawiającego.
19	W przypadku gdy na karcie są 2 PIN-y tj. PIN użytkownika oraz PIN ELP, system powinien zapewnić, że PIN-y te będą miały taką samą wartość.

20	Serwis WWW infrastruktury PKI, musi umożliwiać: zmianę hasła dostępu (zmiana ta dotyczy jednocześnie hasła służącego do uwierzytelniania), wymuszenie zmiany hasła inicjalnego podczas pierwszego logowania do serwisu WWW infrastruktury PKI oraz po resecie hasła wykonanego przez administratora, zażądanie wygenerowania nowego certyfikatu przez użytkownika serwisu. W momencie żądania wydania nowego certyfikatu zostaje unieważniony stary certyfikat, funkcje które związane są z dostępem do karty procesorowej, są osiągalne na jednostce roboczej wyposażonej w czytnik kart inteligentnych. W przeciwnym przypadku musi pojawić się komunikat o niemożliwości wykonania operacji. Powyższe funkcje powinny być wykonywane z poziomu przeglądarki Microsoft Internet Explorer.
21	Oprogramowanie administracyjne dla PKI umożliwia zarządzanie ELP w infrastrukturze klucza publicznego (PKI)