

# Opis Przedmiotu Zamówienia

Testy bezpieczeństwa

## Informacje dotyczące zamówienia

### 1. Zamawiający

Instytut Badań Edukacyjnych

ul. Górczewska 8, 01-180 Warszawa

### 2. Wstęp

Instytut Badań Edukacyjnych w Warszawie (IBE) jest placówką badawczą prowadzącą interdyscyplinarne badania naukowe nad funkcjonowaniem i efektywnością systemu edukacji w Polsce. Jednym z projektów systemowych realizowanych przez IBE na zlecenie Ministerstwa Edukacji Narodowej współfinansowanych ze środków Unii Europejskiej, jest projekt pod nazwą “Prowadzenie i rozwój Zintegrowanego Rejestru Kwalifikacji (etap 2)” (projekt ZRK2).

Zintegrowany Rejestr Kwalifikacji wraz z aplikacjami towarzyszącymi stanowi ważne narzędzie systemowe służące realizacji polityki uczenia się przez całe życie. Pełni ono ważną rolę w integracji funkcjonujących w kraju systemów kształcenia: oświaty i szkolnictwa wyższego oraz obszaru edukacji pozaformalnej i nieformalnego uczenia się.

ZRK gromadzi i udostępnia informacje na temat możliwych do uzyskania w Polsce kwalifikacji spełniających określone przez państwo (w ustawie) wymagania dotyczące m.in. standardu opisu kwalifikacji, przypisania poziomu PRK oraz zasad zapewniania jakości kwalifikacji. ZRK jest rejestrem publicznym w rozumieniu ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne.

ZRK jest rejestrem jawnym, a informacje o kwalifikacjach w nim gromadzone są powszechnie dostępne za pośrednictwem strony internetowej (portalu internetowego) w językach polskim i angielskim. Portal oferuje możliwość łatwego przeszukiwania, porządkowania i agregowania informacji. Portal polskiego rejestru, podobnie jak portale pozostałych krajów UE, będzie powiązany z portalem Europejskiej Ramy Kwalifikacji (ERK).

IBE, od stycznia 2018 r. jest instytucją pierwszego wyboru, do którego zwracają się różne instytucje lub osoby z pytaniami dotyczącymi ZRK. Grupy osób zainteresowanych informacjami zawartymi w ZRK to np. uczniowie, pracownicy,

pracodawcy, nauczyciele, doradcy zawodowi, administracja państwowa, jednostki samorządu terytorialnego, organizacje pracodawców, związki zawodowe, izby gospodarcze, itd.

Podmiot prowadzący rejestr jest naturalnym punktem kontaktowym dla tych grup.

Rejestr pełni funkcję „jednego okienka” dla instytucji składających wnioski. Zadania ZRK wynikające z ustawy o ZSK to m.in.:

1. Dokonywanie wpisów w ZRK i ich aktualizacji.
2. Formalna ocena wniosków: o włączenie kwalifikacji rynkowych do ZSK, o przywrócenie kwalifikacji rynkowej statusu kwalifikacji funkcjonującej, o nadanie uprawnień do certyfikowania kwalifikacji, o wpis na listę podmiotów uprawnionych do pełnienia funkcji zewnętrznego zapewniania jakości. Wnioski składane są wyłącznie drogą elektroniczną.
3. Prowadzenie portalu ZSK w części dotyczącej ZRK.
4. Gromadzenie, przechowywanie i udostępnianie ministrom właściwym, ministrowi koordynatorowi oraz Radzie Interesariuszy raportów i sprawozdań IC oraz PZZJ.
5. Gromadzenie informacji o: liczbie wydanych dokumentów potwierdzających nadanie poszczególnych kwalifikacji, wysokości opłat i przychodów za walidację i certyfikowanie.
6. Zapewnienie dostępu do informacji o Zintegrowanym Rejestrze Kwalifikacji, w szczególności za pośrednictwem Internetu.
7. Monitorowanie funkcjonowania ZRK.
8. Uzupełnianie informacji o wpisanych do ZRK kwalifikacjach o krótkie charakterystyki kwalifikacji w języku angielskim.

System informatyczny ZRK został zaprojektowany w IBE w latach 2013 - 2015 i uruchomiony w środowisku testowym w 2015 r., jeszcze przed wejściem w życie ustawy regulującej zasady działania ZRK (ustawa o ZSK). Rejestr został uruchomiony w lipcu 2016 r. W latach 2018 - 2020 w IBE trwały prace nad modernizacją systemu informatycznego ZRK oraz stworzeniem aplikacji towarzyszących.

## Przedmiot zamówienia

Przedmiotem zamówienia jest przeprowadzenie przez Wykonawcę na rzecz Zamawiającego testów bezpieczeństwa dla 7 aplikacji/narzędzi.

Na dzień ogłaszania zamówienia istnieje jedna aplikacja, która może być poddana testom: CAS oraz jedna aplikacja, która jest w fazie instalacji: aplikacja "Kompas". Pozostałe 5 aplikacji/narzędzi jest w fazie projektowania lub też dopiero będą w fazie projektowania.

Wykonawcą testów bezpieczeństwa nie powinien być dostawca danej aplikacji/narzędzia ani też podmiot od niego zależny

Celem realizowanego zamówienia jest zapewnienie wysokiego poziomu bezpieczeństwa aplikacji objętych testami, które będą odporne na ataki.

Testy będą podzielone na 7 etapów i wykonane zgodnie z wytycznymi z pkt. 1-3 "Zakres prac"

Aplikacje na których będą przeprowadzane testy bezpieczeństwa:

1. CAS (Centralny System Uwierzytelniania)
2. aplikacja "Miasto karier"
3. portal "małe ZRK"
4. aplikacja "Kompas"
5. Narzędzie do automatycznego wspomaganie doradztwa
6. Aplikacja dla uprzywilejowanych użytkowników ułatwiająca opisywanie kwalifikacji i przypisywanie im poziomu PRK
7. Narzędzie ułatwiające tworzenie odwołań do ZSK i kwalifikacji w ogłoszeniach o pracę

Planuje się uruchomienie aplikacji na serwerach w chmurze obliczeniowej lub stacjonarnie.

## Zakres prac

1. Testy penetracyjne typów: "white-box", "black-box" dla wszystkich wymienionych aplikacji WWW w oparciu o metodykę OWASP (Open Web application Security Project) ASVS 4.0 a w szczególności:
  - walidację parametrów,
  - podatność na wstrzyknięcie w przeglądarkę fragmentu kodu np. javascript, który może być uruchomiony w przeglądarce tzw. Cross-Site Scripting (XSS)
  - sprawdzenie mechanizmów uwierzytelniających pod kątem próby ich przełamania (ataki słownikowe i siłowe na hasła, ataki z wykorzystaniem SQL Injection/Blind SQL Injection),
  - próbę przejęcia kontroli nad aplikacją,
  - podatność na ataki techniką Google Hacking,
  - bezpieczeństwo zarządzania kluczami API,
  - weryfikacja czy hasła, integracje z bazami danych i systemami zewnętrznymi zarządzane są w bezpieczny sposób i nie zawarte w kodzie źródłowym lub przechowywane w repozytoriach
  - podatność aplikacji na możliwość nieautoryzowanego przerwania i/lub zakłócenia ciągłości działania (ataki Dos), z wyłączeniem ataków DDoS,
  - ochrona przed enumeracją zasobów oraz haseł,
  - podatność na atak Forcefull browsing,
  - podatność na atak Path Traversal,
  - podsłuchiwanie sesji i kradzież ciasteczek HTTP (zmuszenie przeglądarki ofiary do wykonania pewnej nieautoryzowanej akcji (wykonania requestu HTTP)),
  - badanie podatności aplikacji na możliwość nieautoryzowanego ujawnienia kodu źródłowego,

- badanie podatności aplikacji na możliwość nieautoryzowanego wykonania poleceń systemowych (ataki typu Remote Code Execution)
  - podatność na atak Shell injection,
  - testy mechanizmów zarządzania sesją (m.in. obsługa parametrów sesji przez aplikacje: pliki Cookies), próby podszywania się pod zalogowanego użytkownika, weryfikacja mechanizmów wygaszania sesji, weryfikacja istnienia podatności typu CSRF
  - fuzzing
2. Testy penetracyjne infrastruktury informatycznej systemu ZRK zgodnie z metodyką PTES (The Penetration Testing Execution Standard) w tym m.in.:
- weryfikację dostępności portów TCP/UDP dla hostów systemu ZRK (skanowanie portów), zwłaszcza dla protokołu ipv6,
  - ataki na bazy danych (SQL Injection, Blind SQL Injection, XML Injection, SOAP Injection)
  - sprawdzenie rodzaju, wersji oraz konfiguracji wykorzystywanego oprogramowania systemowego i usługowego,
  - sprawdzenie podatności hostów na ataki w warstwie systemowej,
  - badanie podatności hostów na możliwość dostępu do zasobów plikowych osoby nieuprawnionej,
  - badanie podatności hostów na próby łamania haseł

Testem objęte będą wyznaczone przez Zamawiającego adresy IP (maksymalnie 12)

3. Analizę konfiguracji serwerów na których są aplikacje pod kątem bezpieczeństwa, która będzie obejmowała:
- w przypadku bazy danych: weryfikację aktualności oprogramowania bazy danych, analizę zastosowanych metod uwierzytelniania, sprawdzenie polityki haseł, sprawdzenie mechanizmów przechowywania haseł, logowania zdarzeń, archiwizacji danych, analizę i ocenę mechanizmów kontroli dostępu fizycznego i logicznego,

- w przypadku serwera WWW: weryfikację aktualności oprogramowania serwera, analiza i ocena sposobu obsługi błędów, analizę metod kontroli dostępu fizycznego i logicznego, weryfikację obecności domyślnych kont użytkowników, weryfikację sposobu zarządzania serwerem, ocenę mechanizmów archiwizacji danych

## OPIS APLIKACJI

### Technologie aplikacji

Ze względu na to, że 5 aplikacji jest obecnie lub będzie dopiero w fazie projektowania - nie ma wystarczająco szczegółowych informacji o nich.

Biorąc jednak pod uwagę to, iż Zamawiający posiada infrastrukturę informatyczną opartą o model LAMP (Linux-Debian, Apache, MySQL, PHP) lub LAPP(Linux-Debian, Apache, PostgreSQL, PHP) oraz część aplikacji webowych stworzonych przy użyciu frameworku Laravel to nie zakłada się, iż stworzone aplikacje webowe będą oparte o inny model czy też framework.

### CAS (Centralny System Uwierzytelniania)

Aplikacja wykonana w technologii webowej dostępna pod adresem [cas.ibe.edu.pl](http://cas.ibe.edu.pl). Działa poprawnie w pięciu najpopularniejszych rodzajach przeglądarek (Microsoft Edge / Internet Explorer, Firefox, Chrome, Safari, Opera). Wykorzystuje protokół CAS.

Podstawowym zadaniem aplikacji jest umożliwienie logowania się do pozostałych narzędzi/aplikacji będących w infrastrukturze ZRK a także przypisywanie ról użytkownikom, które następnie zwracane są do pozostałych narzędzi objętych funkcjonalnością logowania przez CAS

Technologie zastosowane w aplikacji to: HTML5, CSS3, Bootstrap, JS (wraz z bibliotekami JQuery i JQuery UI).

### APLIKACJA “MIASTO KARIER”

Planuje się stworzenie **aplikacji** „miasto karier” przeznaczonej dla dzieci i młodzieży, pokazującej w **dostosowanej do wieku** atrakcyjnej formie graficznej, na podstawie danych rejestrowych, wybrane zawody z ich opisami i informacjami powiązanymi.



"Miasto karier" ma być animowanym i interaktywnym narzędziem poszerzającym wiedzę odbiorców w zakresie rynku pracy i zawodów, **pozwalającym zrozumieć młodym odbiorcom powiązania między zawodami.**

Portal powinien zostać przygotowany w postaci izometrycznego rzutu miasta, mapy pozwalającej poprzez wybór budynku (np. sąd) na wyświetlenie postaci będących przykładami zawodów utożsamianych z danym budynkiem (np. sędzia).

Całość narzędzia powinna pozwalać na intuicyjne przeglądanie z poziomu przeglądarki zawartości i pozwolić zrozumieć dzieciom i młodzieży powiązania na rynku pracy, a w konsekwencji wesprzeć planowanie ich przeszłości zawodowej.

Portal będzie wymagał powiązania aplikacji wykonanej w przeważającej części w technologii JavaScript z bazą danych małego ZRK, zawierającego opisy kwalifikacji przygotowane z myślą o dzieciach i młodzieży.

Aplikacja nie będzie miała modułu logowania dla użytkowników. Zakłada się tylko logowanie do panelu administratora aplikacji przez zewnętrzny system CAS. Obsługiwana będzie wyłącznie jedna rola: administrator.

## **PORTAL "MAŁE ZRK"**

Będzie to portal WWW pozwalający uczniom w różnym wieku aktywnie korzystać z ZSK, w tym porównywać kwalifikacje odzwierciedlające różne umiejętności dzieci i młodzieży oraz planować ścieżki uczenia się w oparciu o kwalifikacje.

Ze względu na różne zainteresowania i potrzeby dzieci oraz młodzieży w różnym wieku „małe ZRK” zostanie dostosowane do trzech grup wiekowych: 1) klasy 0-3 szkoły podstawowej; 2) klasy 4-8 szkoły podstawowej; 3) szkoły średniej.

Wszystkie wybrane kwalifikacje rynkowe i zawodowe w rzemiośle zostaną przedstawione w atrakcyjnej i dopasowanej do wieku formie graficznej wraz z dostosowanymi opisami tych kwalifikacji. Planowane jest stworzenie 3 różnych wersji graficznych dostosowanych do wybranej grupy wiekowej.

Aplikacja nie będzie miała modułu logowania dla użytkowników. Zakłada się tylko logowanie do panelu administratora aplikacji przez zewnętrzny system CAS. Obsługiwana będzie wyłącznie jedna rola: administrator.

## Aplikacja “Kompas”

Aplikacja otwarta “Kompas” skierowana jest do szerokiego grona odbiorców. Ilustruje zależności między kwalifikacjami Zintegrowanego Rejestru Kwalifikacji, celem jej jest pomoc w wybieraniu różnorodnych dróg rozwoju zawodowego lub dalszej drogi kształcenia. Aplikacja w sposób graficzny przedstawia grupowanie kwalifikacji ZRK, zbierając podobne kwalifikacje ze względu na branże oraz na podobieństwo charakterystyk i zestawów efektów uczenia się.

Aplikacja pozwala na:

- przeglądanie list kwalifikacji zebranych w branży
- przeglądanie list kwalifikacji przyporządkowanych dziedzinom w ramach branż
- przeglądanie szczegółowych informacji o kwalifikacjach zawodowych

Dostęp do strony z aplikacją “Kompas” jest publiczny, nie wymaga logowania się oraz nie udostępnia konta użytkownika.

Testem nie są objęte aplikacje do których się odnosi ze strony głównej czyli: “Szkolnictwo branżowe” czy też “Zintegrowany Rejestr Kwalifikacji”.

Dane na temat kwalifikacji pobierane są za pomocą API ZRK strony [rejestr.kwalifikacje.gov.pl](http://rejestr.kwalifikacje.gov.pl)

Na stronie głównej znajduje się wyszukiwarka kwalifikacji, wstępne ustawienie filtrów oraz pole wyboru dziedzin zbierających kwalifikacje podobne.

Każdą wyszukaną kwalifikację można kliknąć i przejść w jej szczegóły jako kolejna podstrona.

Na stronie głównej znajduje się też formularz zgłaszania błędów w aplikacji przez Użytkownika. Formularz jest dostępny na wszystkich podstronach

Ze strony głównej można również eksplorować grupy kwalifikacji w formie kafelków, gdzie kliknięcie w poszczególny kafelek z jakąś grupą kwalifikacji można kliknąć w kolejny, aby przejść do bardziej szczegółowych podgrup, aż do wyświetlenia poszczególnych kwalifikacji.

### EKRAN GŁÓWNY


Na stronie głównej znajduje się wyszukiwarka kwalifikacji, wstępne ustawienie filtrów oraz pole wyboru dziedzin zbierających kwalifikacje podobne. Poniżej można wyszukiwać i przeglądać kwalifikacje rynkowe.



**KOMPAS** Sukces i dobro branżowe Zintegrowany Rejestr Kwalifikacji

## Właściwy kierunek Twojego rozwoju

Szukasz pracy, chcesz się przekwalifikować lub uzyskać dodatkową kwalifikację? Skorzystaj z naszego kompasu kwalifikacji.




### Szukaj kwalifikacji

Wpisz szukaną frazę w pole wyszukiwania  
Użyj filtrów, aby dynamicznie ograniczyć rezultaty wyszukiwania

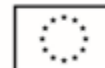
Wybierz   **Wyszukaj**

### Eksploruj grupy kwalifikacji




Przejrzyj informacje o kwalifikacjach zgodnie z ich przynależnością do grup branż.

Wybierz  **Wskaz**




Nauki ścisłe i przyrodnicze (5 grup)	Sport, turystyka i rekreacja (1 grupa)	Kultura i sztuka, moda (10 grup)	Budownictwo i architektura (10 grup)	Metody oceny, transport i logistyka (6 grup)
Nauki o Ziemi, gospodarka i ochrona środowiska (3 grupy)	Business i marketing (3 grupy)	Gastronomia i hotelarstwo (2 grupy)	Śmiertelność i administracja (5 grup)	Handel i sprzedaż (2 grupy)
Nauki humanistyczne i społeczne (10 grup)	Edukacja i szkolenia (3 grupy)	Technika, budownictwo, przemysł (12 grup)	IT i technologie cyfrowe (8 grup)	
Technika, przemysł, inżynieria (10 grup)	Stawianie, budownictwo, prawo (3 grupy)	Uroda (2 grupy)	Opieka zdrowotna (10 grup)	
	Usługi opiekuńcze i społeczne (8 grup)	Bezpieczeństwo mienia i osób (6 grup)		


## Kwalifikacje rynkowe



**Zarządzanie i inżynieria produkcji** – Inżynierowie  
Elektrycy, m. in. Inżynieria Kształtowania i Kształtowania –  
3-letniego stopnia



**Opieka zdrowotna z elementami optometrii** –  
Inżynierowie Kształtowania i Kształtowania w Toruniu –  
3-letniego stopnia



**Wzrostowość** – Analitycy Laboratorium i Zarządzanie  
w Warszawie – 6-letniego stopnia

**O aplikacji**

Aplikacja kampania jest skierowana do szerokiego grona odbiorców do odwołania. Jej celem jest przede wszystkim informowanie o możliwościach edukacji w zakresie kwalifikacji rynkowych. Aplikacja kampania jest skierowana do szerokiego grona odbiorców do odwołania. Jej celem jest przede wszystkim informowanie o możliwościach edukacji w zakresie kwalifikacji rynkowych.

**Pomóż nam ulepszać aplikację**

Zgłoś problem, błąd lub sugestie. Jeśli masz uwagi, napisz nam wiadomość lub zgłoś błąd. Jeśli masz uwagi, napisz nam wiadomość lub zgłoś błąd. Jeśli masz uwagi, napisz nam wiadomość lub zgłoś błąd.

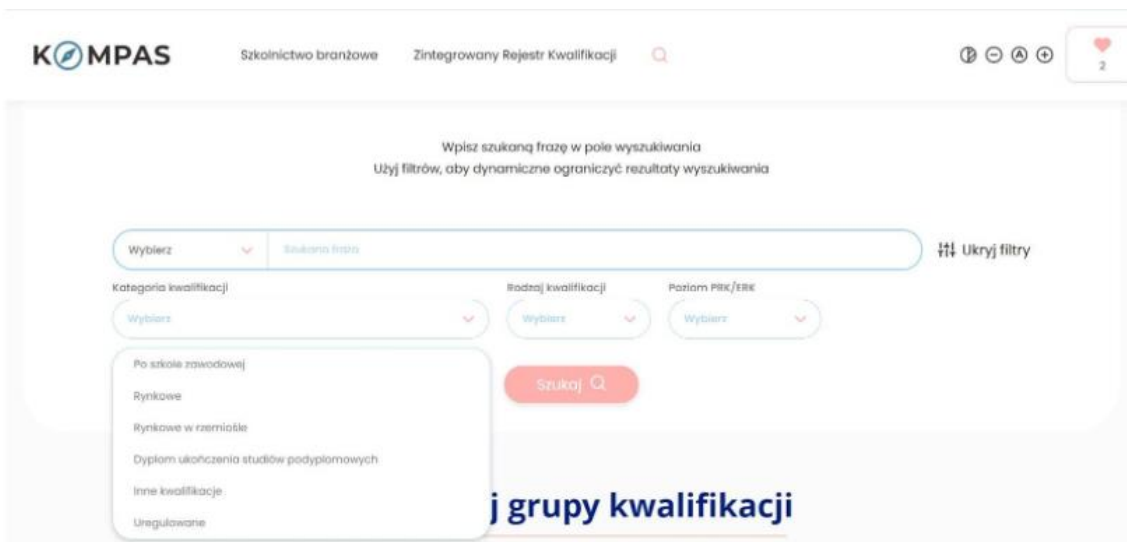
[Opowiedz nam](#) (17)

**Kontakt**

Zintegrowany Rejestr Kwalifikacji  
tel. +48 22 348 71 85  
mail: rejestr@zrk.gov.pl  
www.rejestr.zawodowcy.gov.pl

## EKRAŃ GŁÓWNY – WIDOK FILTRÓW

Na stronie głównej można ograniczyć wyszukiwanie wg filtrów: kategoria kwalifikacji, rodzaj kwalifikacji, poziom PRK/ERK, oraz poprzez wybranie "szukanej frazy". Ostatnie wyszukiwanie ogranicza się filtrami: nazwa kwalifikacji, charakterystyka, efekty uczenia się, słowa kluczowe.



## EKRAN GŁÓWNY – FORMULARZ ZGŁASZANIA BŁĘDU

Widok formularza zgłaszania błędu w aplikacji przez Użytkownika. Formularz jest dostępny na wszystkich podstronach.



## EKRAN GŁÓWNY – WIDOK WYBRANEJ GRUPY KWALIFIKACJI

Widok aplikacji po wybraniu jednej z 20 dziedzin. Przedstawia kolejny podział na grupy kwalifikacji wyodrębnione dla niej oraz liczbę podrup w każdej grupie.

## Eksploruj grupy kwalifikacji



Przełączaj informacje o kwalifikacjach zgodnie z ich przynależnością do grup branż.

Wyszukiwanie

Ustawienia

Nauki humanistyczne i społeczne (0 grup)

Socjologia (4 grup)			
Orientalistyka (10 grup)	Media i dziennikarstwo (6 grup)	Historia i archeologia (4 grup)	Filologie i kulturoznawstwo (94 grup)
Filozofia, etyka i kognitywistyka (4 grup)			
Religie i religioznawstwo (5 grup)	Komunikacja międzykulturowa (6 grup)	Sztuka pisanie i krytyka literacka (4 grup)	Architektura informacji (5 grup)

### WIDOK SCHOWKA

Widok przedstawia schowek wraz z kwalifikacjami dodanymi do niego przez Użytkownika. W Schowku jest również wyszukiwarka kwalifikacji. Schowek jest dostępny na każdej podstronie aplikacji.

## Schowek

Lista Twoich ulubionych kwalifikacji w jednym miejscu. Przeglądaj, dodawaj i usuwaj kwalifikacje łatwo i szybko.



Szukaj kwalifikacji



Wyczyść schowek



Nazwa kwalifikacji	Usuń
Optyka okularowa z elementami optometrii – Uniwersytet Mikołaja Kopernika w Toruniu – pierwszego stopnia	
Zarządzanie i inżynieria produkcji – Uniwersytet Rolniczy im. Hugona Kołłątaja w Krakowie – drugiego stopnia	

Pokaż

5



### WIDOK WYBRANEJ KWALIFIKACJI – KARTA CHARAKTERYSTYKI

Karta charakterystyki wybranej kwalifikacji przedstawia:

- rodzaj kwalifikacji
- poziom PRK/ERK
- opis kwalifikacji ze zdjęciem
- kwalifikacje poprzedzające lub składowe
- kwalifikacje podobne



Sztuka pisanie – Uniwersytet Śląski w Katowicach – pierwszego stopnia

Rodzaj kwalifikacji: pełna Poziom PRK/ERK: 5 Wyświetl w ZRK

Ogólna charakterystyka  
Możliwości zdobycia kwalifikacji  
Perspektywy zatrudnienia  
Zarobki


### Opis kwalifikacji

Tytuł zawodowy: licencjat Profil studiów: ogólnoakademicki Forma prowadzenia studiów: stacjonarne Język studiów: polski Czas trwania studiów - liczba semestrów: 6 Liczba punktów ECTS: 180 ISCED: Literatura i językoznawstwo (lingwistyka)


### Kwalifikacje poprzedzające lub składowe

Świadectwo dojrzałości


### Podobne kwalifikacje



Socjologia – Uniwersytet im. Adama Mickiewicza w Poznaniu – drugiego stopnia



Socjologia – Uniwersytet Śląski w Katowicach – drugiego stopnia



### Pomóż nam ulepszać aplikację

Znalazłeś funkcjonalność w aplikacji, która Twoim zdaniem nie działa jak należy? Pomóż nam rozwiązać ten problem. Zgłoś sugestię lub błąd w aplikacji! Każda taka uwaga jest dla nas wyjątkowo cenna i pomaga rozwijać produkt jeszcze lepiej dostosowany do Twoich potrzeb!

Zgłoś błąd

## Narzędzie do automatycznego wspomaganie doradztwa

Będzie to tzw. “Wirtualny Asystent” - Narzędzie do automatycznego wspomaganie doradztwa (czatbot), który będzie działać na nowym portalu ZRK

<https://kwalifikacje.gov.pl/k>

Czatbot będzie skierowany do wielu grup użytkowników, nie będzie wymagał od nich logowania.

“Wirtualny Asystent” będzie aplikacją gromadzącą zapytania i/lub przebieg całych konwersacji z użytkownikami. Dostęp do samej aplikacji będzie odbywał się poprzez proste



uwierzytelnianie dla administratora (podanie loginu, najlepiej adresu e-mail i hasła) w Panelu Administracyjnym. Nie będzie wymagane profilowanie uprawnień.

Więcej informacji na temat narzędzia dostępne pod linkiem:

<https://bip.ibe.edu.pl/index.php/zamowienia-publiczne/1772-ogloszenie-o-zamiarze-przeprowadzenia-wstepnych-konsultacji-rynkowych-wirtualny-asystent>

## **Aplikacja dla uprzywilejowanych użytkowników ułatwiająca opisywanie kwalifikacji i przypisywanie im poziomu PRK**

Aplikacja webowa skierowana do konkretnych grup użytkowników: ekspertów IBE, pracowników ministerstw, instytucji certyfikujących i szkół wyższych. Będzie to aplikacja wspierająca opisywanie kwalifikacji, porównywanie kwalifikacji z innymi i ułatwiająca podejmowanie decyzji o kształcie, jakości i włączeniu kwalifikacji do systemu. Dostęp do aplikacji będzie wymagał uwierzytelnienia (np. poprzez CAS).

## **Narzędzie ułatwiające tworzenie odwołań do ZSK i kwalifikacji w ogłoszeniach o pracę**

Otwarta aplikacja webowa, niewymagająca uwierzytelniania użytkowników. Będzie to aplikacja umożliwiająca przeglądanie bazy ZRK w poszukiwaniu informacji o kwalifikacjach i efektach uczenia się możliwych do wykorzystania w ogłoszeniach o pracę, np. ze względu na rodzaj wykształcenia lub zakładane umiejętności.

## Sposób realizacji zamówienia

1. Termin realizacji: dzień podpisania umowy - marzec 2023.
2. W ciągu 10 dni roboczych od podpisania umowy w siedzibie Zamawiającego odbędzie się pierwsze spotkanie konsultacyjne, na którym zostanie ustalony zakres prac i szczegółowe warunki realizacji zamówienia oraz współpracy Wykonawcy z Zamawiającym.

Kolejne spotkania konsultacyjne odbywać się będą po wdrożeniu nowych aplikacji, jednak nie później niż 5 dni roboczych od zainicjowania spotkania przez Zamawiającego. Zamawiający może zdecydować się przeprowadzenie spotkania w formie zdalnej

3. Po spotkaniu w ciągu 5 dni roboczych Wykonawca przygotuje "Plan testów" dla danego etapu uwzględniając wymagania z przedmiotu zamówienia.
4. Po wykonaniu każdego testu dotyczącego wybranego etapu realizacji zamówienia Wykonawca sporządzi raport. Raport będzie zawierał m.in.:
  - szczegółowy opis przeprowadzonych prac,
  - szczegółowy wykaz wykrytych podatności, wraz z dowodami na ich istnienie w postaci zrzutów ekranu oraz logów oprogramowania użytego podczas audytu
  - każda podatność powinna być oznaczone kodem ze słownika CVE (Common Vulnerabilities and Exposures),
  - rekomendacje w zakresie sposobu wyeliminowania wykrytych podatności wraz z podaniem zaleceń i instrukcji do wprowadzenia korekt konfiguracyjnych w celu ich eliminacji,
  - opis w formie streszczonej aktualnego poziomu bezpieczeństwa wraz z jego oceną
  - raport powinien być zabezpieczony przed możliwością przejęcia i odczytania zawartości przez podmioty niebiorące udziału w realizacji przedmiotu umowy

Wykonawca ma 20 dni roboczych na wykonanie każdego etapu testów i sporządzenie raportu

5. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanego przez Wykonawcę raportu o którym mowa w pkt. 4 "Sposób realizacji zamówienia" w terminie 10 dni roboczych od otrzymania każdego raportu.
6. Wykonawca zobowiązany jest do uwzględnienia w raporcie uwag wniesionych przez Zamawiającego w terminie 5 dni roboczych.
7. Formuła realizacji zamówienia zostanie określona w uzgodnieniu z Wykonawcą w trakcie spotkań roboczych po podpisaniu umowy.
8. Zamawiający zapłaci tylko za zlecone na etapie realizacji zamówienia testy aplikacji a całkowite wynagrodzenie Wykonawcy może ulec stosownemu zmniejszeniu, jeżeli Zamawiający zrezygnuje ze stworzenia pozostałych 5 aplikacji.

## Warunki realizacji zamówienia

1. Zamówienie realizowane będzie przez osobę lub osoby posiadające wiedzę i doświadczenie adekwatne do wykonania testów bezpieczeństwa w oparciu o najbardziej aktualne metody jego naruszeń wraz z udokumentowanymi certyfikatami bezpieczeństwa informacji.
2. Prace realizowane w ramach zamówienia będą prowadzone z uwzględnieniem potrzeb Zamawiającego.
3. Wykonawca dołoży wszelkich starań do uwzględnienia ważnych elementów mogących mieć wpływ na naruszenie bezpieczeństwa systemu ZRK nie wymienionych w przedmiocie zamówienia a dotyczących testów penetracyjnych aplikacji WWW, infrastruktury ZRK oraz analizy konfiguracji serwerów ZRK.
4. Realizacja przedmiotu zamówienia odbywać się będzie głównie zdalnie, niemniej jednak w uzasadnionych przypadkach Zamawiający akceptuje realizację zleconych prac w siedzibie Zamawiającego. Realizacja zleconych zadań będzie wymagać obecności Wykonawcy w siedzibie Zamawiającego, jeżeli zdalna realizacja będzie niemożliwa lub może negatywnie wpływać na jakość wykonania zlecenia jednostkowego.
5. Realizując zlecenie Wykonawca zweryfikuje całość udostępnionego kodu nie stosując próbkowania
6. Wykonawca oddeleguje do nadzorowania umowy osobę, która będzie zatrudniona przez wykonawcę. Osoba ta będzie odpowiedzialna m.in. za:
  - a) przestrzeganie terminów umownych dotyczących Wykonawcy,
  - b) kontakty z Zamawiającym, w tym przekazywanie odpowiedzi na pytania Zamawiającego dotyczące realizacji umowy,

- c) przestrzeganie obowiązków Wykonawcy wynikających z umowy, w szczególności dotyczących zapisów odnośnie danych osobowych i poufności informacji.

## Harmonogram płatności

Płatność za każdy etap realizacji zamówienia nastąpi po ostatecznym zaakceptowaniu przez Zamawiającego raportu z przeprowadzonych testów bezpieczeństwa.