**LTC Sp. z o.o. siedziba**
ul. Narutowicza 2, 98-300 Wieluń
NIP 8270007803
REGON 005267185

KRS 0000196558
Kapitał zakładowy 2 000 000 PLN
Sąd Rej. Łódź-Śr. XX Wydział KRS

**LTC Sp. z o.o. dział sprzedaży i usług**
ul. Pabianicka 159/161, 93-490 Łódź
tel. (42) 206 66 01
tel. (42) 206 66 07, 206 66 09

www.finn.pl
biuro@finn.pl

Załącznik nr 1 do Zapytania ofertowego nr iEZD.Z1/2023

# Opis Przedmiotu Zamówienia do Zapytania ofertowego pn. „Merytoryczne prace badawczo – rozwojowe podwykonawcy”

Zapytanie ofertowe prowadzone jest w celu wyłonienia podwykonawcy prac badawczo-rozwojowych, których wykonanie jest niezbędne w realizacji projektu „Inteligentne Elektroniczne Zarządzanie Dokumentami” ubiegającego się o wsparcie w ramach programu Fundusze Europejskie dla Nowoczesnej Gospodarki, Priorytet I. Wsparcie dla przedsiębiorców, Działanie Ścieżka SMART.

**Zamawiający**

LTC Sp. z o.o.
ul. Narutowicza 2
98-300 Wieluń
NIP 8270007803

Wieluń, dnia 26.04.2023r.

# Spis treści

# 1 Ogólne informacje o projekcie

Projekt obejmuje przeprowadzenie badań przemysłowych oraz prac rozwojowych, których efektem będzie system Inteligentnego Elektronicznego Zarządzania Dokumentami (iEZD). Oferowany przez wnioskodawcę od kilkunastu lat system elektronicznego zarządzania dokumentami FINN EZD dla administracji publicznej zostanie rozbudowany o nowe inteligentne aplikacje, które z wykorzystaniem uczenia maszynowego oraz technik przetwarzania języka naturalnego udostępnią inteligentne funkcje:

- analizy znaczeniowej z ekstrakcją danych,
- klasyfikacji oraz
- semantycznego wyszukiwania dokumentów.

Utworzona zostanie również samodzielna wersja aplikacji iEZD na potrzeby integracji z rozwiązaniami innych dostawców (np. EZDRP) za pośrednictwem API.

Istotą innowacyjności rezultatów projektu będą efektywne i wiarygodne algorytmy i modele ML zapewniające przetwarzanie dokumentów na podstawie ich zawartości merytorycznej. Zasadniczą kwestią jest również zapewnienie narzędzi oraz procesów monitorowania, walidacji i aktualizacji zapewniających utrzymanie sprawności modeli uczenia maszynowego wykorzystywanych w środowisku produkcyjnym.

W rezultacie iEZD zautomatyzuje czynności związanych z rejestracją, przekazywaniem/dekretowaniem oraz obsługą dokumentów u klientów wnioskodawcy.

Rezultaty badań przemysłowych i prac rozwojowych zostaną wdrożone w działalności biznesowej LTC i wejdą w skład nowych i znacząco ulepszonych systemów informatycznych. Opracowane zostaną również bezpieczne i efektywne procedury aktualizowania inteligentnych algorytmów systemu iEZD.

Przeprowadzone badania przemysłowe oraz eksperymentalne prace rozwojowe, obejmujące również testy w środowisku demonstracyjnym oraz produkcyjnym u rzeczywistych klientów, doprowadzą do powstania innowacyjnych produktów, co najmniej na skalę krajową, które mają potencjał do wykształcenia nowego rynku systemów inteligentnego przetwarzania dokumentów w administracji publicznej.

# 2 Podział projektu na zadania

Przedmiot zamówienia obejmuje realizację merytorycznych prac badawczo-rozwojowych w ramach poszczególnych zadań realizowanego projektu:

| Zadanie | Opis | Docelowy poziom TRL | Realizacja od | Realizacja do |
|---|---|---|---|---|
| Zadanie 1 | Opracowanie inteligentnych algorytmów bazowych, budowa i uczenie modeli ML. Wstępna integracja algorytmów na poziomie laboratoryjnym. | TRL IV | 2023-10-01 | 2024-09-30 |
| Zadanie 2 | Podniesienie efektywności inteligentnych algorytmów, rozbudowa i uczenie modeli ML, określenie ostatecznych wartości hiperparametrów, integracja algorytmów w warunkach laboratoryjnych odwzorowujących z dużą wiernością warunki rzeczywiste. | TRL VI | 2024-10-01 | 2025-09-30 |
| Zadanie 3 | Opracowanie komponentów aplikacyjnych, optymalizacja inteligentnych algorytmów, testy na danych rzeczywistych, tuning parametrów, douczanie modeli ML. | TRL VII | 2025-10-01 | 2026-03-31 |
| Zadanie 4 | Docelowa integracja rozwiązań, testy w środowisku produkcyjnym. | TRL IX | 2026-04-01 | 2026-09-30 |

Prace podwykonawcy realizowane będą w każdym zadaniu odpowiednio do zakresu realizowanych prac przedstawionego poniżej.

# 3 Specyfikacja zakresu zamówienia

Ogólnym celem realizacji zamówienia jest zapewnienie wysokiego poziomu bezpieczeństwa opracowywanych rozwiązań, ze szczególnym uwzględnieniem charakterystyki podmiotów administracji publicznej. Wysoki poziom zagrożenia w domenie cyberbezpieczeństwa, a także wysokie wymagania w zakresie ochrony danych osobowych oraz poufności (m.in. tajemnica przedsiębiorstwa, tajemnica skarbowa) stawiają wysokie wymagania wobec systemów funkcjonujących w administracji publicznej. W szczególności dotyczy to systemów elektronicznego zarządzania dokumentami (czyli tzw. systemów klasy EZD), w których pracują wszyscy pracownicy jednostki. W systemie EZD są zatem przetwarzane wszystkie dokumenty wpływające i powstające w urzędzie (z wyłączeniem dokumentów przetwarzanych w kancelarii tajnej).
W związku z tym opracowywany w ramach projektu system aplikacji iEZD musi spełniać wysokie wymagania bezpieczeństwa, a także nie może wpływać negatywnie na bezpieczeństwo systemów EZD z którymi będzie współpracował.
Szczegółowy zakres prac wykonawcy w ramach poszczególnych zadań przedstawiono poniżej.

## 3.1 Zadanie 1: Opracowanie inteligentnych algorytmów bazowych, budowa i uczenie modeli ML. Wstępna integracja algorytmów na poziomie laboratoryjnym

1. Świadczenie przez cały okres realizacji zadania konsultacji w zakresie:
    a. bezpieczeństwa informacji w odniesieniu do opracowywanych algorytmów oraz komponentów aplikacyjnych,
    b. zagrożeń cyberbezpieczeństwa oraz sposobu im zapobiegania,
    c. protokołów sieciowych, standardów wymiany danych, technik kryptograficznych,
    d. programowych i sprzętowych mechanizmów zabezpieczeń,
2. Analiza bezpieczeństwa opracowywanych w ramach zadania algorytmów i modeli ML.
3. Symulacje komputerowe w zakresie bezpieczeństwa oraz niezawodności opracowywanych w ramach zadania algorytmów AKD (algorytmy klasyfikacji i dekretacji), AIW (algorytmy indeksowania i wyszukiwania), AED (algorytmy ekstrakcji danych).
4. Badania w zakresie metod zapewnienia zasad dostępu do obiektów i danych systemu EZD przez algorytmy AED, AKD, AIW.
5. Badania w zakresie zapobiegania wyciekowi danych (w tym danych osobowych) do modeli ML.
6. Badania w zakresie opracowania bezpiecznych, zgodnych z prawem mechanizmów współdzielenia wytrenowanych modeli ML, ich aktualizacji, dystrybucji i doskonalenia.

## 3.2 Zadanie 2: Podniesienie efektywności inteligentnych algorytmów, rozbudowa i uczenie modeli ML, określenie ostatecznych wartości hiperparametrów, integracja algorytmów w warunkach laboratoryjnych odwzorowujących z dużą wiernością warunki rzeczywiste

1. Świadczenie przez cały okres realizacji zadania konsultacji w zakresie:
    a. bezpieczeństwa informacji w odniesieniu do opracowywanych algorytmów oraz komponentów aplikacyjnych,
    b. zagrożeń cyberbezpieczeństwa oraz sposobu im zapobiegania,
    c. protokołów sieciowych, standardów wymiany danych, technik kryptograficznych,
    d. programowych i sprzętowych mechanizmów zabezpieczeń,
2. Analiza bezpieczeństwa opracowywanych w ramach zadania algorytmów i modeli ML.
3. Symulacje komputerowe w zakresie bezpieczeństwa oraz niezawodności opracowywanych w ramach zadania algorytmów AKD (algorytmy klasyfikacji i dekretacji), AIW (algorytmy indeksowania i wyszukiwania), AED (algorytmy ekstrakcji danych).
4. Badania w zakresie metod zapewnienia zasad dostępu do obiektów i danych systemu EZD przez algorytmy AED, AKD, AIW.
5. Badania w zakresie zapobiegania wyciekowi danych (w tym danych osobowych) do modeli ML.

6. Badania w zakresie opracowania bezpiecznych, zgodnych z prawem mechanizmów współdzielenia wytrenowanych modeli ML, ich aktualizacji, dystrybucji i doskonalenia.

## 3.3 Zadanie 3: Opracowanie komponentów aplikacyjnych, optymalizacja inteligentnych algorytmów, testy na danych rzeczywistych, tuning parametrów, douczanie modeli ML

1. Świadczenie przez cały okres realizacji zadania konsultacji w zakresie:
    a. bezpieczeństwa informacji w odniesieniu do opracowywanych algorytmów oraz komponentów aplikacyjnych,
    b. zagrożeń cyberbezpieczeństwa oraz sposobu im zapobiegania,
    c. protokołów sieciowych, standardów wymiany danych, technik kryptograficznych,
    d. programowych i sprzętowych mechanizmów zabezpieczeń,
2. Analiza bezpieczeństwa opracowywanych w ramach zadania komponentów aplikacyjnych oraz zoptymalizowanych algorytmów i modeli ML.
3. Symulacje komputerowe w zakresie bezpieczeństwa oraz niezawodności zoptymalizowanych w ramach zadania algorytmów AKD (algorytmy klasyfikacji i dekretacji), AIW (algorytmy indeksowania i wyszukiwania), AED (algorytmy ekstrakcji danych).
4. Testy bezpieczeństwa opracowanych w ramach zadania komponentów aplikacyjnych iEZD.
5. Prace rozwojowe w zakresie metod zapewnienia zasad dostępu do obiektów i danych systemu EZD przez algorytmy AED, AKD, AIW.
6. Prace rozwojowe wraz z testami w zakresie zapobiegania tzw. „wyciekowi danych” (w tym danych osobowych) do modeli ML.
7. Prace rozwojowe wraz z testami w zakresie zabezpieczeń mechanizmów współdzielenia wytrenowanych modeli ML, ich aktualizacji, dystrybucji i doskonalenia.

## 3.4 Zadanie 4: Docelowa integracja rozwiązań, testy w środowisku produkcyjnym

1. Świadczenie przez cały okres realizacji zadania konsultacji w zakresie:
    a. bezpieczeństwa informacji w odniesieniu do opracowywanych algorytmów oraz komponentów aplikacyjnych,
    b. zagrożeń cyberbezpieczeństwa oraz sposobu im zapobiegania,
    c. protokołów sieciowych, standardów wymiany danych, technik kryptograficznych,
    d. programowych i sprzętowych mechanizmów zabezpieczeń,
2. Analiza bezpieczeństwa opracowywanych w ramach zadania komponentów aplikacyjnych oraz zoptymalizowanych algorytmów i modeli ML.
3. Testy bezpieczeństwa i niezawodności opracowanych w ramach zadania komponentów aplikacyjnych iEZD.
4. Testy skuteczności metod zapewnienia zasad dostępu do obiektów i danych systemu EZD przez algorytmy AED, AKD, AIW.
5. Testy skuteczności zapobiegania tzw. „wyciekowi danych” (w tym danych osobowych) do modeli ML.
6. Testy skuteczności zabezpieczeń mechanizmów współdzielenia wytrenowanych modeli ML, ich aktualizacji, dystrybucji i doskonalenia.
7. Testy bezpieczeństwa integracji poszczególnych rozwiązań w środowisku produkcyjnym.

# 4 Wymagane urządzenia / zasoby kadrowe

## 4.1 Wymagane zasoby sprzętowe

### 4.1.1 Wielowarstwowy analizator ruchu sieciowego o wysokiej przepustowości: 1 kpl. Parametry:

1. Obsługa interfejsów w technologii 40GigaEthernet, 10GigaEthernet i 1GigaEthernet.
2. Administracja w oparciu o protokoły: SSH, HTTP/HTTPS, SNMP v1, v2c, v3, SNMP TRAP.
3. Rozbudowane mechanizmy filtrowania ruchu.

4. Język zapytań obejmujące wszystkie warstwy ruchu sieciowego. Kompatybilność z formatem tcpdump/Wireshark.
5. Mechanizmy notyfikacji dla wykrywanych anomalii.
6. Wysokowydajna pamięć nieulotna zapewniająca rejestrację ruchu z wydajnością powyżej 10 gigabitów przez okres co najmniej 5 minut.
7. Pamięć nieulotna zapewniająca rejestrację ruchu z wydajnością powyżej 1 gigabita przez okres co najmniej 8 h.
8. Analizator jest wyposażony w kieszeń umożliwiającą zgrywanie danych na zewnętrzne nośniki SATA 2,5/3,5”. Kieszeń obsługuje zarówno dyski talerzowe HDD oraz pamięciowe SSD.
9. Mechanizm monitorowania obciążenia i zbierania dziennika zdarzeń z urządzeń sieciowych (przełączniki, routery, firewalle). Raportowanie graficzne w różnych wariantach i okresach.
10. Moduł monitorowania obciążenia dla środowisk do wirtualizacji.
11. Moduł monitorowania konfiguracji urządzeń sieciowych.
12. Analizator jest wyposażony w ekran (lub ekrany) o rozdzielczości co najmniej 4 milionów pikseli.
13. Analizator ma umożliwić kompleksową diagnostykę i rozwiązywanie trudnych problemów sieciowych podczas realizacji prac rozwojowych dla zastosowań sieciowych i aplikacyjnych.
14. Analizator ma umożliwiać wykonywanie różnorodnego typu audytów bezpieczeństwa i testów wydajności infrastruktury.
15. W zestawie z zarządzalnym fizycznym wieloportowym przełącznikiem sieciowym.

Analizator umożliwi kompleksową diagnostykę i rozwiązywanie trudnych problemów sieciowych podczas badań i prac rozwojowych prototypów/produktów opisanych powyżej.
Będzie użyty jako istotne ułatwienie podczas wykonywania audytów bezpieczeństwa i testów wydajności infrastruktury systemu sterowania.
Zapewni:

- mechanizmy notyfikacji dla wykrywanych anomalii,
- monitorowania obciążenia i zbieranie dziennika zdarzeń dla środowisk fizycznych i zwirtualizowanych oraz urządzeń sieciowych.

### 4.1.2 Zaawansowany symulator rzeczywistego ruchu sieciowego: 1 kpl. Parametry:

1. Obsługa interfejsów w technologii 40GigaEthernet, 10GigaEthernet i 1GigaEthernet.
2. Administracja w oparciu o protokoły: SSH, HTTP/HTTPS, SNMP v1, v2c, v3, SNMP TRAP.
3. Generowanie ruchu sieciowego ICMP/TCP/UDP w oparciu o popularne profile użytkowe.
4. Generowanie zaawansowanego ruchu sieciowego IPv4/IPv6 w oparciu o zaawansowane algorytmu programowane przy użyciu skryptów i języków programowania.
5. Wysokowydajna pamięć nieulotna o pojemności powyżej 512GB do przechowywania wzorców ruchu o wydajności odczytu powyżej 3GBajtów/s.
6. Pamięć nieulotna umożliwiająca przechowywanie historycznych dzienników generowanego ruchu o pojemności powyżej 6TB.
7. Generowanie ruchu wysokopoziomowego dla testów aplikacyjnych (w tym: testy wydajnościowe baz danych SQL, testy wydajnościowe platform wirtualizacyjnych, testy wydajnościowe serwerów WWW/RESTapi).
8. Możliwość uruchamiania dedykowanych modułów aplikacyjnych do generowania rzeczywistych szablonów ruchu dla dowolnych (w tym przyszłych) protokołów aplikacyjnych. Infrastruktura pisania i uruchamiania modułów powinna uwzględniać co najmniej 4 różne i popularne języki programowania.
9. Tworzenie harmonogramów i zapamiętanych customizacji dla profilów ruchu.
10. Obsługa profilów symulujących problemy sieciowe (przeciążenie sieci, ataki DDoS, DoS, skanowanie sieci).
11. Symulator ma umożliwić kompleksowe i zautomatyzowane przeprowadzanie testów wydajnościowych podczas realizacji prac rozwojowych dla zastosowań sieciowych i aplikacyjnych.
12. Symulator ma umożliwić wykonywanie audytów bezpieczeństwa i wydajności infrastruktury.

Obejmuje platformę sprzętową i oprogramowanie. Zapewnia:

- obsługę interfejsów 1/10/40GigaEthernet,
- symulacje problemów: przeciążenie, ataki DDoS, DoS, incydenty bezpieczeństwa,

- tworzenie harmonogramów i zapamiętanych customizacji dla profilów ruchu testowego.

Symulator współpracuje z Wielowarstwowym analizatorem ruchu.
Symulator umożliwi kompleksowe i zautomatyzowane testy wydajnościowe prototypów/produktów komponentów aplikacyjnych KA, implementujących inteligentne algorytmy AI (adaptacyjne i predykcyjne).
Generowanie ruchu sieciowego ICMP/TCP/UDP w oparciu o popularne profile użytkowe, wsparcie dla IPv4/IPv6, algorytmy programowane przy użyciu skryptów i jęz. programowania,
wysokopoziomowe testy aplikacyjne, testy wydajnościowe, testy baz danych SQL i platform wirtualizacyjnych, testy serwerów WWW/RESTapi.

## 4.2 Wymagane zasoby kadrowe podwykonawcy

1. Wykonawca na czas realizacji zamówienia musi dysponować zespołem co najmniej 2 osób, które będą osobiście uczestniczyć w wykonywaniu zamówienia i które będą posiadały następujące kwalifikacje zawodowe, doświadczenie i wykształcenie oraz zakres wykonywanych czynności:
   a) każda z osób posiada minimum 2-letnie doświadczenie jako wykonawca prac badawczych lub rozwojowych, a przedmiot prac jest zbieżny z celami i przedmiotem niniejszego zamówienia,
   b) co najmniej 1 (jedna) osoba posiada tytuł doktora inżyniera nauk technicznych (lub wyższy),
   c) co najmniej 1 (jedna) osoba przewidziana jest na stanowisko Kierownika projektu, która posiada wykształcenie wyższe, posiada co najmniej 2-letnie doświadczenie w kierowaniu zespołem w co najmniej 2 projektach ICT
   d) członkowie zespołu posiadają sumaryczną wiedzę, doświadczenie i wysokie umiejętności w zakresie:
      - zaplanowanych rozwiązań sprzętowych i aplikacyjnych projektu,
      - realizacji projektów B+R z zaplanowaną komercjalizacją wyników,
      - złożonych systemów informatycznych oraz zaawansowanej elektroniki w pracach projektowych, programistycznych, instalacyjnych, konfiguracyjnych i wdrożeniowych oraz przeprowadzaniu testów,
      - inteligentnych algorytmów,

   Zamawiający dopuszcza łączenie funkcji Kierownika Projektu z innymi funkcjami.

   Kadra Podwykonawcy w działaniach musi uwzględnić przyjęte terminy osiągania poziomu gotowości technologii iEZD, zgodnie z pkt 2 OPZ Podział projektu na zadania.

   Na podstawie opracowanej dokumentacji Projektu oszacowano, że do wykonania przedmiotu prac rozwojowych specjaliści Podwykonawcy będą w każdym kolejnym miesiącu do dyspozycji Zamawiającego w wymiarze czasu odpowiadającemu 2 etatom.
   Uwaga: Zakłada się tolerancję na poziomie 0,5 etatu, przy czym w całym okresie podwykonawstwa średniomiesięczny wymiar nie może być niższy łącznie niż 1,5 etatu.

# 5 Termin wykonania zamówienia

1. Zamówienie realizowane będzie od dnia 01.10.2023 do dnia 30.09.2026 r.
2. Usługi muszą być zrealizowane zgodnie z zatwierdzonym przez Zamawiającego harmonogramem.
3. Płatności będą rozliczane po realizacji usług.