ul. Konstantynowska 79/81
95-200 Pabianice, Poland
https://www.fif.com.pl

Koordynator Projektu
+ 48 602 257 542
projekty@fif.com.pl

NIP 7310005314
REGON 470625813
KRS 0001018980

FIF.F&F K1/2023 OPZ
Opis przedmiotu zamówienia – Zakup licencji i usługi nadzoru autorskiego wdrożenia oprogramowania Rozproszonego, bezpiecznego magazynu danych i centrum certyfikacji (RBMD-CC)

Spis treści

1. Wstęp

Zamówienie dotyczy projektu B+R o nazwie „Środowisko oraz proces projektowania i produkcji inteligentnych, autonomicznych, zminiaturyzowanych urządzeń brzegowych FIF, umożliwiających realizację celów zero-emisyjności oraz poprawy efektywności energetycznej" (akronim projektu: FIF) i jest realizowane w ramach Modułu wdrożenie innowacji, w Zadaniu „Zakup licencji i usług nadzoru autorskiego w zakresie wdrożenia Rozproszonego, bezpiecznego magazynu danych i centrum certyfikacji (RBMD-CC)".

Przedmiot zamówienia obejmuje:

1) Licencja oprogramowania Rozproszonego, bezpiecznego magazynu danych i centrum certyfikacji (RBMD-CC);
2) Nadzór autorski wdrożenia oprogramowania Rozproszonego, bezpiecznego magazynu danych i centrum certyfikacji, obejmujący usługi: instalacji, konfiguracji, parametryzacji i wdrożenia elementów RBMD-CC.

Niniejszy dokument definiuje wymagania dla:

1) dostarczanego oprogramowania Rozproszonego, bezpiecznego magazynu danych i centrum certyfikacji (RBMD-CC);
2) wykonania nadzoru autorskiego wdrożenia oprogramowania, obejmującego w szczególności usługi instalacji, konfiguracji i parametryzacji oraz porady techniczne prowadzące do wszechstronnego wykorzystania rozwiązań RBMD-CC zgodnie z celami projektu.

Rozproszony, bezpieczny magazyn danych i centrum certyfikacji składa się z 2 współpracujących ze sobą elementów:

1) RBMD to uniwersalny komponent zapewniający niezawodną i rozproszoną platformę do przechowywania oraz udostępniania treści i dokumentów cyfrowych.
2) Oprogramowanie CC jest kluczowym elementem systemu bezpieczeństwa. Dokumentacja obejmuje:
   a) Politykę certyfikacji,
   b) Kodeks postępowania certyfikacyjnego,
   c) Procedury planowania, instalacji, uruchomienia i eksploatacji Centrum certyfikacji.

Oprogramowanie RBMD-CC zostanie udostępnione na zasadzie licencji niewyłącznej:

1) z prawem do dowolnego modyfikowania i rozwoju oraz nieograniczonego w czasie i terytorialnie wykorzystania oprogramowania,
2) bez limitu liczby jego użytkowników, systemów, ośrodków certyfikacji i wystawionych certyfikatów,
3) umożliwiająca korzystanie z wszystkich wspieranych przez HSM długości kluczy szyfrujących.

Szczegółowy zakres licencji zawiera Umowa wstępna na dostawę licencji i usług nadzoru autorskiego wdrożenia.

Zakupione licencje i nadzór autorski wdrożenia RBMB-CC muszą zapewnić:

1) Bezpieczeństwo transakcji i zdygitalizowanych dokumentów dotyczących działania w modelach procesów:
   a) Proces projektowania i szczupłej produkcji (PPSP),
   b) Proces eksploatacji i rozwoju (PER).
2) Funkcjonalności i cechy (w tym wskaźniki) opisane w dalszej części dokumentu OPZ.

Wdrożone oprogramowanie RBMD-CC musi zapewnić osiągnięcie celów Zamawiającego, a w szczególności:

1) stanowić wydajną i bezpieczną infrastrukturę przechowywania danych, w sposób rozproszony z zastosowaniem mechanizmów wysokiej dostępności;
2) zapewnić efektywność procesów budowy, wdrażania i eksploatacji bezpiecznych aplikacji wykorzystujących technologię rozproszonego rejestru (typu blockchain) działających w chmurze;
3) integrować wszystkie mechanizmy bezpieczeństwa w ściśle zintegrowanym i jednolitym komponencie zapewniającym kompleksową ochronę danych, pozwalającą na budowanie niezależnych od klastra aplikacyjnego osobnych klastrów przechowywania danych;

4) realizować funkcjonalności zapewniające spełnienie zidentyfikowanych kluczowych cech:
   a) inteligentne wykrywanie anomalii w działaniu klastra;
   b) gwarancja bezpieczeństwa dokumentów, transakcji i procesów biznesowych oraz autentyczności integralności przechowywanych danych;
5) posiadać wbudowane mechanizmy:
   a) zabezpieczania integralności i niezaprzeczalności danych w postaci zintegrowanego rozproszonego rejestru DLT/blockchain;
   b) wykrywania anomalii, w tym mechanizmy inteligentnego wykrywania anomalii w działaniu klastra (algorytmy outlier detection);
6) posiadać opracowane algorytmy kryptograficzne i mechanizmy konsensusu dla rozproszonego rejestru DLT wykorzystujące wyniki wykrywania anomalii, m.in. do automatycznego zabezpieczania przetwarzania danych w poszczególnych węzłach klastra.
7) współpracować ze sprzętowymi modułami bezpieczeństwa (HSM), sieciowym serwerem czasu z odbiornikiem GPS i wzorcem czasu oraz obsługiwać nowoczesne algorytmy zalecane przez eIDAS (funkcje skrótu SHA-256, SHA-512, klucze RSA o długości powyżej 4096 bitów i ECC o długości powyżej 384 bitów);
8) uwzględnić wymagania m.in. norm: PN ISO ISO/IEC 27001, 27002, 27004, 27005, 27010, TS 27017, 27036.

Bezpieczeństwo transakcji i procesów biznesowych to przede wszystkim:

1) zapewnienie niezaprzeczalności wykonywanych operacji kryptograficznych gwarantowane matematycznym dowodem,
2) współpraca z rozwiązaniami centrum certyfikacji w zakresie zapewnienia niezaprzeczalnego potwierdzenia tożsamości,
3) automatyczne zapewnienie niezaprzeczalności podpisów elektronicznych w długim okresie czasu oraz inne mechanizmy umożliwiające długotrwałą archiwizację danych o transakcjach,
4) mechanizm ochrony danych przed niepowołanym dostępem w zdefiniowanym okresie czasu, zrealizowany z wykorzystaniem dedykowanego algorytmu oraz sprzętowego modułu bezpieczeństwa (Hardware Security Module).

Zamawiający (zwany również Wnioskodawcą w kontekście projektu FIF) w oparciu o rozwiązania RBMD-CC przeprowadzi zaplanowane w Module B+R prace rozwojowe, mające cele oraz przedmiot opisane w kolejnym rozdziale Ogólny opis Projektu FIF.

Wdrożenie RBMD-CC zapewni funkcjonalności i możliwości, umożliwiające zaplanowaną już w 2025r. pilotażową sprzedaż produktów oraz usług, wykorzystujących uzyskane wyniki w Module wdrożenie innowacji oraz w Module B+R.

2. Ogólny opis Projektu FIF

Plan projektu zakłada:

1) okres realizacji projektu: 01.07.2024 – 30.10.2027 r.
2) rozpoczęcie realizacji zadań:
   a) w Module B+R od dnia 01.07.2024 r.
   b) w Module wdrożenie innowacji od dnia 01.08.2024 r.
3) wykonanie przedmiotowego zamówienia w okresie od dnia 01.08.2024 r. do dnia 30.09.2024 r.

W przypadku zmiany terminu rozpoczęcie projektu Wykonawca jest zobowiązany wykonać przedmiot zamówienia w nowym terminie, wskazanym przez Zamawiającego, bez prawa sprzeciwu oraz żądania dodatkowej zapłaty.

2.1. Skrócony opis projektu

Przedmiotem i wynikiem zaplanowanych prac rozwojowych będą: nowa rodzina URZĄDZEŃ BRZEGOWYCH FIF w postaci inteligentnych sterowników, agentów, sensorów, aktuatorów, z wbudowaną sztuczną inteligencją (AI/ML) oraz nowy Proces projektowania i szczupłej produkcji (PPSP), umożliwiający masową kastomizację.

Powstaną nowe narzędzia automatyzacji procesu uczenia maszynowego (autoML) oraz Bezpieczne, rozproszone środowisko projektowania, budowy, testowania i wdrożenia oprogramowania (BRŚ), w tym do tworzenia predykcyjnych, adaptacyjnych i uczących się algorytmów (AI/ML), zapewniających w zintegrowanych procesach przemysłowych i biznesowych, ekonomiczność „drogi do zera" przy osiąganiu celu zero-emisyjności oraz poprawy efektywności energetycznej.

Technologię zweryfikuje w warunkach rzeczywistych, wykonanie w środowisku BRŚ: interoperacyjnych protokołów komunikacyjnych, algorytmów AI/ML i pakietu komponentów Oprogramowania urządzeń brzegowych (OUB), wykorzystywanego w rodzinie FIF, zgodnie z Procesem eksploatacji i rozwoju (PER) – w zastosowaniach do inteligentnych wielonośnikowych mikrosieci energetycznych (SMEM).

Cel projektu zostanie osiągnięty, kiedy unikatowa technologia, procedury oraz urządzenia FIF, zdominują komercyjną ofertę produktowo-usługową, zapewniając wieloletnią przewagę konkurencyjną – dzięki efektom innowacji produktowej i procesowej, cyfrowej oraz ekoinnowacji na poziomie krajowym, w tym:

- interoperacyjności i wysokiej wydajności hiperkonwergentnej infrastruktury w skalowalnych modelach przetwarzania brzegowego, mgły obliczeniowej i chmury, z najwyższymi standardami bezpieczeństwa;
- minimalizacji kosztów i czasu zmiany modelu architektury systemu sterowania przy zachowaniu najwyższego poziomu niezawodności i bezpieczeństwa;
- unifikacji i optymalizacji różnych modeli wdrożeniowych infrastruktury systemów sterowania, z gwarancją bezpiecznej zmiany modelu wdrożeniowego infrastruktury;
- elastycznej automatyzacji i autonomizacji „z ludzkim dotykiem".

2.2. Cele Modułu B+R

Celem i przedmiotem prac rozwojowych będą:

1) Predykcyjne, adaptacyjne, uczące algorytmy (AI/ML) oraz narzędzia automatyzacji procesu uczenia maszynowego (autoML).
2) Rodzina urządzeń brzegowych FIF z wbudowanymi AI/ML i system operacyjnym czasu rzeczywistego, w postaci zunifikowanych: sterowników, agentów, sensorów i aktuatorów.
3) Bezpieczne, rozproszone środowisko projektowania, budowy, testowania i wdrożenia oprogramowania (BRŚ) oraz zautomatyzowane i zautonomizowane procesy:
   a) projektowania i szczupłej produkcji (PPSP);
   b) eksploatacji i rozwoju (PER).

Nowa technologia i produkty zapewnią:

1) integrację procesów przemysłowych i biznesowych dla ekonomiczności osiągania zero-emisyjności oraz poprawy efektywności energetycznej;
2) interoperacyjność, bezpieczeństwo, niezawodność i wydajność hiperkonwergentnej infrastruktury w skalowalnych modelach przetwarzania brzegowego, mgły obliczeniowej i chmury;
3) masową kastomizację FIF;
4) efektywność usług wdrożenia i wsparcia klientów FIF.

2.3. Cele Modułu wdrożenie innowacji

Zakupione licencje: Centrum certyfikacji (CC) i Rozproszonego, bezpiecznego magazynu danych i centrum certyfikacji (RBMD-CC) oraz usługi nadzoru autorskiego ich wdrożenia, spełnią wymagania procesów PPSP i PER oraz wynikających z nich zautomatyzowanych i zautonomizowanych procedur. Zostaną wykorzystane do opracowania środowiska BRŚ i rodziny urządzeń brzegowych FIF implementujących algorytmy AI/ML.

PPSP, PER, BRŚ i FIF poddane audytom weryfikującym zgodność z normami, wdrożone dla specjalistów i klientów Wnioskodawcy oraz jego Partnerów biznesowych, zapewnią:

1) projektowanie, budowę, testowanie i wdrażanie hiperkonwergentnych oraz skalowalnych systemów sterowania opartych na algorytmach AI/ML integrujących zarządzanie przemysłowe i biznesowe oraz optymalizujących i racjonalizujących wykorzystanie OZE;
2) gwarancje synchroniczności pomiaru i integralności przetwarzanych wielomodalnych danych przemysłowych, energetycznych i biznesowych;
3) wysoką wieloletnią konkurencyjność oraz zyskowność oferty usługowo-produktowej.

3. Licencja oprogramowania Rozproszonego, bezpiecznego magazynu danych i centrum certyfikacji (RBMD-CC)

3.1. Wymagania dotyczące licencji

Szczegółowy zakres licencji zawiera Umowa wstępna na dostawę licencji i usług nadzoru autorskiego wdrożenia.

3.2. Analiza zidentyfikowanych kluczowych cech BRMD

3.2.1. Efektywność procesów wykorzystujących technologię rozproszonego rejestru działających w chmurze i mgle obliczeniowej

Efektywność to przede wszystkim skrócenie czasu potrzebnego na wykonanie czynności w ramach procedur:

1) wynikających z Procesu projektowania i szczupłej produkcji (PPSP) dotyczącego rodziny urządzeń brzegowych FIF;
2) dotyczących działań z wykorzystaniem Bezpiecznego, rozproszonego środowisko projektowania, budowy, testowania i wdrożenia oprogramowania (BRŚ).

Kluczowymi funkcjonalnościami RBMD będzie gwarantowane przechowywanie oraz bezpieczne udostępnianie danych plikowych i obiektowych. Jego zadaniem będzie zapewnienie ochrony autentyczności i integralności oraz nienaruszalność dokumentów i dzienników zdarzeń w sposób wydajny, bezpieczny i odporny na błędy programisty. RBMD musi zapewniać wszechstronna platformę przechowywania danych dla budowy bezpiecznych aplikacji biznesowych działających w chmurze i mgle obliczeniowej.

Kompletny RBMD w oparciu o blockchain lub DLT zdejmie z programisty konieczność dokładnej znajomości zagadnień rozproszonego rejestru, dzięki czemu szybciej zostaną uzyskane rezultaty w postaci na przykład:

1) opracowania zamówionej dedykowanej wersji oprogramowani urządzeń FIF,
2) obsługi dokumentacji wynikającej z czynności projektowania i wykonywania nowych algorytmów AI/ML, interfejsów i funkcji oprogramowaniu układowego urządzeń FIF.

3.2.2. Inteligentne wykrywanie anomalii w działaniu klastra

Adaptacyjne algorytmy muszą zapewniać możliwość wykrycia anomalii będących skutkiem:

1) naruszenia integralności infrastruktury klastra lub komponentów zewnętrznych,
2) ataków oraz aktów cyberprzestępczości,
3) nieoptymalnej lub błędnej konfiguracji komponentów aplikacyjnych działających w klastrze, sieci wewnętrznych oraz innych komponentów klastra,
4) konfliktów w konfiguracji poszczególnych usług i elementów składowych,
5) błędów w samym oprogramowaniu realizującym usługi w klastrze.

Algorytmy automatycznie muszą dostosowywać profile monitorowania wykorzystania poszczególnych zasobów oraz profile ruchu sieciowego wewnątrz klastra do aktualnego stanu uruchomionych usług. Adaptacyjność algorytmów jest kluczowa dla uzyskania wiarygodnych wyników monitorowania. Wartością dodaną RBMD będzie automatyzacja czynności diagnostycznych z użyciem inteligentnych algorytmów wykrywania anomalii. Pozwoli to na wcześniejsze wykrywanie potencjalnych zagrożeń mogących skutkować utratą ciągłości działania usług realizowanych w oparciu o klaster. Identyfikacja przypadków nieefektywnego przepływu danych wewnątrz klastra pozwoli na optymalizację poszczególnych usług biznesowych. Algorytmy będą się charakteryzować reagowaniem na wykryte anomalie, które w przypadku wykrycia anomalii obniżą zdolność danego węzła do uczestniczeniu w głosowaniu nad konsensusem. Przełoży się to bezpośrednio na eliminację wielu powszechnie znanych zagrożeń dla wdrożeń technologii DLT takich jak: Partition Attack, Delay Attack, DDoS, Sybil Attack, Time-Jacking Attack, Race Attack, Finney Attack.

3.2.3. Gwarancja bezpieczeństwa transakcji i procesów biznesowych

Bezpieczeństwo transakcji i procesów biznesowych to przede wszystkim:

1) zapewnienie niezaprzeczalności wykonywanych operacji kryptograficznych gwarantowane matematycznym dowodem,
2) współpraca z rozwiązaniami centrum certyfikacji w zakresie zapewnienia niezaprzeczalnego potwierdzenia tożsamości,
3) automatyczne zapewnienie niezaprzeczalności podpisów elektronicznych w długim okresie czasu oraz inne mechanizmy umożliwiające długotrwałą archiwizację danych o transakcjach,
4) mechanizm ochrony danych przed niepowołanym dostępem w zdefiniowanym okresie czasu, zrealizowany z wykorzystaniem dedykowanego algorytmu oraz sprzętowego modułu bezpieczeństwa (Hardware Security Module).

3.3. Wymagania ogólne BRMD

1) Przedmiotem dostawy są licencje oprogramowania rozproszonego, bezpiecznego magazynu danych transakcyjnych i biznesowych (RBMD).
2) RBMD stanowić będzie wydajną i bezpieczną infrastrukturę przechowywania danych. RBMD musi integrować wszystkie mechanizmy bezpieczeństwa w ściśle zintegrowanym i jednolitym komponencie zapewniającym kompleksową ochronę danych. Ma pozwolić na budowanie niezależnych od klastra aplikacyjnego osobnych klastrów przechowywania danych.
3) RBMD musi realizować funkcjonalności zapewniające spełnienie zidentyfikowanych kluczowych cech:
   a) efektywność procesów budowy, wdrażania i eksploatacji bezpiecznych aplikacji wykorzystujących technologię rozproszonego rejestru działających w chmurze,
   b) inteligentne wykrywanie anomalii w działaniu klastra,
   c) gwarancję bezpieczeństwa dokumentów, transakcji i procesów biznesowych.
4) Dostarczane licencje muszą obejmować wszystkie funkcjonalności wymagane wobec RBMD.
5) RBMD posiada wbudowane mechanizmy zabezpieczania integralności i niezaprzeczalności danych w postaci zintegrowanego rozproszonego rejestru DLT/blockchain.
6) RBMD posiada wbudowane mechanizmy wykrywania anomalii.
7) RBMD musi posiadać mechanizmy inteligentnego wykrywania anomalii w działaniu klastra (algorytmy outlier detection).
8) RBMD musi posiadać opracowane algorytmy kryptograficzne i mechanizmy konsensusu dla rozproszonego rejestru DLT wykorzystujące wyniki wykrywania anomalii.
9) RBMD ma umożliwiać przechowywanie danych w sposób rozproszony z zastosowaniem mechanizmów wysokiej dostępności

3.4. Wymagania szczegółowe BRMD

3.4.1. Wykrywanie anomalii

1) Wykrywane anomalie muszą obejmować zdarzenia/zjawiska:
   a) naruszenia integralności infrastruktury klastra lub komponentów zewnętrznych,
   b) ataków oraz aktów cyberprzestępczości, w szczególności:
      i) Partition Attack,
      ii) Delay Attack,
      iii) DDoS,
      iv) Sybil Attack,
      v) Time-Jacking Attack,
      vi) Race Attack,
      vii) Finney Attack.
   c) nieoptymalnej lub błędnej konfiguracji:
      i) klastra jako całości,

   ii) jego komponentów,
   iii) usług realizowanych w klastrze,
   d) błędów w oprogramowaniu komponentów klastra oraz usług realizowanych w klastrze,
   e) konfliktów pomiędzy usługami realizowanymi w klastrze jak również konfliktach pomiędzy usługami realizowanymi w klastrze i komponentami klastra.
2) Zastosowane algorytmy sztucznej inteligencji muszą umożliwić wykrywanie zarówno anomalii jednokryterialnych, które identyfikowane są zmianą (miarą) jednego parametru jak również anomalii wielokryterialnych, które możliwe są do wykrycia jedynie z wykorzystaniem wielu miar jednocześnie.
3) Algorytmy powinny koncentrować się na wykryciu anomalii, czyli odstępstw od normalnego działania, bez względu na ich pochodzenie. Oznacza to, że będzie realizowane wykrywanie nietypowych wartości danych. Działanie algorytmu nie jest ukierunkowane na wykrycie konkretnego schematu, co umożliwia wykrycie również „nienauczonych" ataków czy błędów.
4) RBMD musi umożliwiać zbieranie i analizę parametrów, które wykazują dużą korelację z występowaniem anomalii, a następnie wykorzystanie sztucznej inteligencji do ich wykrywania w czasie rzeczywistym.
5) Algorytmy automatycznie muszą dostosowywać profile monitorowania wykorzystania poszczególnych zasobów oraz profile ruchu sieciowego wewnątrz klastra do aktualnego stanu uruchomionych usług. Adaptacyjność algorytmów jest kluczowa dla uzyskania wiarygodnych wyników monitorowania.
6) RBMD musi zapewniać możliwość analizy anomalii w klastrach realizujących chmurę prywatną.
7) RBMD musi posiadać zaimplementowane efektywne algorytmy kryptograficzne realizujące operacje:
   a) weryfikację podpisów elektronicznych/pieczęci elektronicznych/znaczników czasu,
   b) podpisywanie/znakowanie czasem z wykorzystaniem urządzeń HSM,
   c) konserwację podpisów elektronicznych,
   d) szyfrowanie / deszyfrowanie obiektów i plików.
8) Inteligentne algorytmy muszą brać pod uwagę charakterystykę rozwiązań działających w modelu mikrousługowym w klastrze:
   a) rozproszone przetwarzanie i przechowywanie danych na wiele węzłów działających w klastrze lub poza nim,
   b) adaptacyjne algorytmy przydziału zasobów klastra oraz skalowania ilości instancji poszczególnych mikrousług (tzw. pod'ów),
   c) dynamiczne mechanizmy sterowania ruchem wewnątrzklastrowym.
9) Wykrywanie anomalii musi obejmować szeroko rozumianą analizę parametrów charakteryzujących stan poszczególnych węzłów oraz mikrousług.
10) Wykrywanie nieprawidłowości w klastrze należy oprzeć o wielokryterialną analizę parametrów charakteryzujących stan klastra.
11) Wykrywanie anomalii musi obejmować:
   a) naruszenia integralności węzłów klastra, w tym m.in.:
      i) dostęp do węzła (konsoli),
      ii) operacje na demonie kubelet,
      iii) operacje na komponentach klastra (serwer API, scheduler, controller manager),
   b) naruszenia bezpieczeństwa sieci, w tym m.in.:
      i) nietypowy przepływ ruchu wewnątrzklastrowego,
      ii) ekspozycja usług poza klaster,
   c) naruszenia integralności usług działających w klastrze, w tym m.in.:
      i) dostęp do kontenera usługi z poziomu innej usługi,
      ii) ekspozycja portów,
      iii) wysycanie zasobów węzła (tym samym tzw. „głodzenie" pozostałych usług).
12) Inteligentne algorytmy wykrywania anomalii powinny wykorzystywać do uczenia się informacje o zdarzeniach (sieciowych, autoryzacji, transakcjach biznesowych) gromadzone w rozproszonych rejestrach.

3.4.2. Wbudowane mechanizmy rozproszonego rejestru DLT

1) RBMD w ramach mechanizmów ochrony klastra musi przechować w rozproszonym rejestrze:
   a) obrazy kontenerów aplikacyjnych,
   b) konfiguracje kontenerów aplikacyjnych,
   c) obrazy komponentów klastra,
   d) konfiguracje komponentów klastra.
2) Technologia rozproszonego rejestru powinna zostać zaimplementowana z wykorzystaniem algorytmów i mechanizmów konsensusu, bazujących na danych o anomaliach występujących w poszczególnych węzłach. To podejście pozwoli na zwiększenie wydajności funkcji konsensusu bez utraty wysokiego poziomu odporności CFT (Crash Faut Tolerance) oraz BFT (Byzantium Fault Tolerance).
3) Algorytm konsensusu powinien być uruchamiany za każdym razem, gdy do rejestru zapisywana jest transakcja i od jego zakończenia uzależniona jest propagacja tejże transakcji na poszczególne węzły klastra.
4) RBMD musi uwzględniać integrację z klastrem sprzętowych modułów bezpieczeństwa HSM (samych z siebie działających w klastrze niezawodnościowym) oraz serwerów czasu, mogących służyć jako TSA („time stamping authority").
5) Zagadnienia zapewnienia autentyczności i integralności komponentów klastra i aplikacji uruchamianych na klastrze uwzględniają odpowiednie rozwiązania takie jak: analiza wewnątrzklastrowego ruchu sieciowego pomiędzy poszczególnymi usługami, czy też potwierdzanie w rozproszonym rejestrze autentyczności obrazów kontenerów przed ich uruchomieniem.
6) Istotnym zagadnieniem jest minimalizacja obciążenia poszczególnych komponentów klastra komponentami RBMD (węzły weryfikacyjne, węzły klienckie, itp.).
7) Zaimplementowane algorytmy kryptograficzne musza pozwolić na zagwarantowanie spójności metadanych kryptograficznych z chronionymi danymi.
8) RBMD musi zapewnić gwarancję integralności, autentyczności oraz nienaruszalności danych, a także wiarygodne mechanizmy weryfikacji tych gwarancji.
9) Wszelkie operacje muszą być niezaprzeczalnie odnotowywane w dzienniku zdarzeń, również chronionym przed modyfikacją.
10) Samo środowisko RBMD (klaster aplikacyjny lub dedykowany klaster przechowywania danych) będzie również chroniony mechanizmami ochrony klastra.

3.5. Specyfikacja minimalnych wymagań technicznych oprogramowania CC

1) Przedmiotem dostawy są licencje oprogramowania Centrum certyfikacji (CC).
2) Oprogramowanie CC jest kluczowym elementem systemu bezpieczeństwa.
3) Oprogramowanie CC musi być zainstalowane i wstępnie skonfigurowane w terminie nie późniejszym niż pierwszy miesiąc realizacji Zadania Z.EK.7
4) Oprogramowanie CC musi:
   a) współpracować ze sprzętowymi modułami bezpieczeństwa (HSM), sieciowym serwerem czasu z odbiornikiem GPS i wzorcem czasu;
   b) obsługiwać nowoczesne algorytmy zalecane przez eIDAS (funkcje skrótu SHA-256, SHA-512, klucze RSA o długości powyżej 4096 bitów i ECC o długości powyżej 384 bitów).
5) Pełna integracja ze sprzętowym modułem bezpieczeństwa HSM (certyfikat bezpieczeństwa wg normy FIPS-140-2 na poziomie 2 i 3).
6) Możliwość uruchomienia instalacji testowej bez konieczności posiadania HSM oraz w trybie programistycznej symulacji HSM.
7) Automatyczna obsługa repozytorium certyfikatów, list CRL, usługi OCSP, znakowania czasem TSA.
8) Możliwość pracy w trybie podwyższonego bezpieczeństwa (tzw. tryb off-line).
9) Współpraca z klastrami wielu urządzeń HSM w celu uzyskania wysokiej dostępności (HA) i w celu skalowania wydajności.
10) Procedury planowania, instalacji, uruchomienia i eksploatacji Centrum Certyfikacji.
11) Dokumentacja zgodna z zaleceniami RFC 3647.

12) Oprogramowanie ma zostać wdrożone w instancji testowej bez wykorzystania HSM oraz w instancji produkcyjnej z wykorzystaniem HSM. Wdrożenie musi obejmować opracowanie kompletnej dokumentacji i procedur pracy dla CC (w szczególności polityka certyfikacji, kodeks certyfikacyjny, repozytorium OID).
13) Oprogramowanie sieciowych usług składania i weryfikacji podpisu zgodna z EIDAS (EIDAS)
    a) Składanie i weryfikacja podpisów elektronicznych zgodnych ze standardami eIDAS.
    b) Zgodność ze standardami ETSI: EN 319 102, EN 319 132, EN 319 172, EN 319 312, TS 119 612.
    c) Formaty podpisów elektronicznych: XADES, PADES, CADES oraz ASiC.
    d) Obsługa list dostawców usług zaufania (TSL).
    e) Weryfikacja certyfikatów na podstawie list CRL oraz za pomocą usługi OCSP.
    f) Weryfikacja certyfikatów kwalifikowanych i niekwalifikowanych.
    g) Weryfikacja: podpisów elektronicznych, pieczęci elektronicznych oraz znaczników czasu. Obejmuje weryfikację podpisu profilem zaufanym.
    h) Architektura: usługi w modelu mikrousług uruchamianych w środowisku wirtualizacji na poziomie systemu operacyjnego (operating system level virtualization) – tzw. kontenery Docker.
    i) Współpraca z klastrami wielu urządzeń HSM w celu uzyskania wysokiej dostępności (HA) i w celu skalowania wydajności.
    j) Obsługa IPv4 i IPv6. Zgodność z protokołami HTTP/HTTPS oraz RESTful. Pełne wsparcie w zakresie wykorzystania zewnętrznych serwerów typu proxy i reverse proxy.
    k) Możliwość wykorzystania sprzętowego modułu bezpieczeństwa HSM (protokoł PKCS#11 lub CSP).

3.6. Wymagania w zakresie dokumentacji Polityki certyfikacji i Kodeksu postępowania certyfikacyjnego

1) Z oprogramowaniem CC musi być dostarczona dokumentacja obejmująca:
    a) Politykę certyfikacji, zwanej dalej Polityką,
    b) Kodeks postępowania certyfikacyjnego, zwanego dalej Kodeksem,
    c) Procedury planowania, instalacji, uruchomienia i eksploatacji Centrum certyfikacji.
2) Dokumentacja wskazana powyżej musi być dostarczona w terminie instalacji i wstępnej konfiguracji oprogramowania CC.
3) Polityka określa ogólne zasady świadczenia usług zaufania, w tym techniczne i organizacyjne rozwiązania, wskazujące sposób, zakres oraz warunki tworzenia i stosowania certyfikatów.
    a) Polityka określa proces świadczenia usług zaufania oraz jego uczestników.
    b) Szczegółowy opis zawiera dokument: Kodeks postępowania certyfikacyjnego, zwany dalej Kodeksem. Definicje pojęć użytych w Polityce są określone w Kodeksie.
    c) Usługi zaufania w zakresie wydawania zaufanych certyfikatów niekwalifikowanych, zwanych dalej Certyfikatami, realizuje Zamawiający w ramach Centrum certyfikacji.
4) Zakres zastosowania Polityki:
    a) Polityka jest stosowana do wydawania i zarządzania certyfikatami wydawanymi przez Zamawiającego. Przez certyfikat należy rozumieć elektroniczny plik poświadczony elektronicznie przez Zamawiającego, w którym klucz publiczny jest przyporządkowany do subskrybenta i umożliwia jego identyfikację.
    b) Certyfikaty, wydawane zgodnie z Kodeksem, nie są certyfikatami kwalifikowanymi. Podpis elektroniczny weryfikowany przy pomocy tych certyfikatów nie wywołuje skutków prawnych równorzędnych podpisowi własnoręcznemu.
    c) Certyfikaty opisane w Polityce są generowane przez urząd certyfikacji (Root CC) prowadzony przez Zamawiającego. Root CA jest urzędem pierwszego poziomu, który wydaje certyfikat dla samego siebie (tzw. certyfikat samopodpisany), wystawia certyfikaty dla subskrybentów oraz udostępnia informacje niezbędne do weryfikacji ważności wydanych przez siebie certyfikatów. Zadania związane z przyjmowaniem wniosków o wydanie/zawieszenie lub unieważnienie certyfikatów, oraz z wydawaniem certyfikatów realizują Operatorzy albo świadczone są elektronicznie przez samoobsługowy system informatyczny.
    d) Certyfikaty mogą zawierać dane i służyć do identyfikacji innych podmiotów niż osoby fizyczne.

e) Odpowiedzialność Zamawiającego, w tym finansowa, odpowiedzialność subskrybenta, odbiorcy usług zaufania oraz strony ufającej jest określona w Kodeksie

5) Minimalny zakres zagadnień przewidzianych w dokumencie Polityka certyfikacji:
   a) Certyfikaty.
   b) Świadczenie usług zaufania.
   c) Subskrybent.
   d) Strona ufająca.
   e) Zmiany polityk.
6) Kodeks określa szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki tworzenia i stosowania certyfikatów.
   a) Kodeks definiuje również strony biorące udział w procesie świadczenia usług zaufania, odbiorców usług oraz podmioty wykorzystujące certyfikaty, ich prawa oraz obowiązki.
   b) Kodeks jest stosowany do wydawania i zarządzania zaufanymi certyfikatami niekwalifikowanymi wydawanymi Zamawiającego, w ramach Centrum Certyfikacji.
   c) Kodeks został stworzony na podstawie zaleceń RFC 3647 (Certificate Policy and Certification Practice Statement Framework) i ma na celu zaspokajać potrzeby informacyjne wszystkich uczestników infrastruktury PKI opisanej w przedmiotowym dokumencie i obsługiwanej przez Zamawiającego.
   d) Ogólne zasady postępowania stosowane przez Zamawiającego przy świadczeniu usług zaufania są opisane w dokumencie Polityka certyfikacji. Szczegóły dotyczące realizacji zasad opisanych w Polityce są zawarte w przedmiotowym Kodeksie
7) Minimalny zakres zagadnień przewidzianych w dokumencie Kodeks postępowania certyfikacyjnego.
   a) Odpowiedzialność za publikowanie i gromadzenie informacji.
   b) Identyfikacja i uwierzytelnienie.
   c) Wymagania dla uczestników infrastruktury PKI w cyklu życia certyfikatu.
   d) Procedury bezpieczeństwa fizycznego, operacyjnego i organizacyjnego.
   e) Procedury bezpieczeństwa technicznego.
   f) Profil certyfikatu i listy CRL.
   g) Audyt zgodności i inne oceny.
   h) Inne kwestie biznesowe i prawne.

4. Nadzór autorski wdrożenia oprogramowania Rozproszonego, bezpiecznego magazynu danych i centrum certyfikacji, obejmujący usługi: instalacji, konfiguracji, parametryzacji i wdrożenia elementów RBMD-CC

Nadzór autorski wdrożenia oprogramowania rozproszonego, bezpiecznego magazynu danych i centrum certyfikacji (RBMD-CC) obejmujący usługi: instalacji, konfiguracji, parametryzacji elementów RBMD-CC oraz wdrożenia wielopoziomowych mechanizmów bezpieczeństwa, ma zapewnić gwarancję poufności oraz autentyczności danych i dokumentów przechowywanych w systemie elektronicznych rejestrów, formularzy i repozytoriów.

Nadzór autorski wdrożenia stanowi opisane w budżecie Projektu koszty usług doradczych.

Wykonane usługi w okresie nie dłuższym niż 2 miesiące w formie co najmniej 8 wizyt jednego specjalisty w czasie 8h w lokalizacji Zamawiającego i zdalne czynności techniczne wykonane w łącznym czasie co najmniej 256h, muszą:

1) Zagwarantować szybki czas i skuteczność wdrożenia RBMD-CC;
2) Zaplanować wdrożenie uwzględniając zagadnienia:
   a) Wybór wymaganych podsystemów;
   b) Definiowanie hierarchii CA (Centrów Certyfikacji);
   c) Planowanie domen bezpieczeństwa;
   d) Określenie wymagań dotyczących certyfikatów podsystemu;
   e) Planowanie bezpieczeństwa sieciowego i fizycznego;
   f) Tokeny do przechowywania kluczy i certyfikatów podsystemów systemu certyfikacji;
   g) Listra kontrolna planowania Infrastruktury Klucza Publicznego (PKI);
   h) Opcjonalne usługi dostarczane przez strony trzecie;
3) Umożliwić bezpośrednie uczestnictwo w czynnościach wdrożenia wszystkim specjalistom Zamawiającego;
4) Pozwolić bezpośrednio zgłaszać uwagi do twórcy oprogramowania i szybko eliminować stwierdzone wady RBMD-CC;
5) Opracować materiały szkoleniowe dla użytkowników w zakresie „Wprowadzenie do infrastruktury klucza publicznego”:
   a) Szyfrowanie i deszyfrowanie;
   b) Podpisy cyfrowe;
   c) Certyfikaty i uwierzytelnianie;
   d) Cykl życia certyfikatu;
   e) Zarządzanie kluczami;
6) Opracować materiały szkoleniowe dla administratorów w zakresie „Wprowadzenie do CC”:
   a) Przegląd podsystemów;
   b) Podsystemy składowe systemu certyfikacji;
   c) Architektura systemu certyfikacji;
   d) PKI;
   e) Zarządzanie kartami chipowymi (inteligentnymi);
   f) Usługi CC;
   g) Klonowanie.

Terminy wizyt w lokalizacji Zamawiającego powinny być dostosowane do postępów wdrożenia, z właściwym zaplanowaniem godzin w zakresie zdalnych czynności technicznych i porad. Zamawiający powinien uwzględniać terminy sugerowane przez Zamawiającego, zgłaszane w wyprzedzeniem co najmniej 7-dniowym.

Wizyta powinna obejmować działania wykonywane przez min. 1 specjalistę w czasie ok. 6-8h. Zdalne konsultacje powinny być wykonywane telefonicznie oraz przy pomocy komunikatorów preferowanych przez Zamawiającego. Zamawiający i Wykonawca powinny dążyć do partnerskiego modelu współpracy oraz wspólnie kształtować

organizacyjne i techniczne warunki jej wykonywania. W przypadku sporów ostateczne decyzje będą należeć do Zamawiającego.

Zaplanowany 2-miesięczny okres wdrożenia i liczba 256h wykonywania usługi, powinny być wystarczające dla osiągnięcia celów wskazanych w rozdziale „Wstęp" oraz prowadzić do uzyskania efektywności działań.

W sytuacji potrzeby zwiększenia zaplanowanej liczby godzin, Zamawiający i Wnioskodawca powinni preferować zdalne czynności techniczne oraz minimalizować liczbę zdecydowanie droższych wizyt bezpośrednich w lokalizacji Wnioskodawcy (np. z uwagi na koszty dojazdów i noclegów).

Plan projektu zakłada:

1) rozpoczęcie realizacji zadań:
   a) w Module B+R od dnia 01.07.2024 r.
   b) w Module wdrożenie innowacji od dnia 01.08.2024 r.
2) wykonanie przedmiotowych usług w okresie od dnia 01.08.2024 r. do dnia 30.09.2024 r.

W przypadku zmiany terminu rozpoczęcie projektu Wykonawca jest zobowiązany wykonać przedmiot zamówienia w nowym terminie, wskazanym przez Zamawiającego, bez prawa sprzeciwu oraz żądania dodatkowej zapłaty.