Opis Przedmiotu Zamówienia

Cz. I – Audyt bezpieczeństwa i wydajności systemów teleinformatycznych MRiT – PEF, ST SDG PL, PI\_PZ

1. Przedmiot zamówienia

Przedmiotem zamówienia jest wykonanie audytów bezpieczeństwa i wydajności systemów teleinformatycznych wraz z usługą wsparcia eksperckiego inżyniera bezpieczeństwa IT zgodnie ze specyfikacją w poszczególnych rozdziałach.

Na przedmiot zamówienia składają się następujące zadania:

1. Wykonanie I fazy audytu bezpieczeństwa i wydajności Systemu Technicznego Jednolitego Portalu Cyfrowego (ST SDG PL).
2. Wykonanie II fazy audytu bezpieczeństwa i wydajności Systemu Technicznego Jednolitego Portalu Cyfrowego (ST SDG PL) po optymalizacji systemu.
3. Przeprowadzenie audytu bezpieczeństwa systemów teleinformatycznych Platformy Elektronicznego Fakturowania: aplikacji Brokera PEF, Książki Adresowej PEF i Portalu efaktura.gov.pl.
4. Przeprowadzenie testów cyberbezpieczeństwa i wydajności nowych modułów funkcjonalnych Platformy Internetowej Polityki Zakupowej Państwa – prawo opcji.
5. Realizacja doraźnych zleceń wsparcia w zakresie cyberbezpieczeństwa dot. systemów teleinformatycznych MRiT – prawo opcji.

Umowa zostanie zawarta na okres 24 miesięcy. Orientacyjny harmonogram zadań znajduje się w rozdz. V OPZ.

1. Opis systemów
2. System Techniczny Jednolitego Portalu Cyfrowego

System (ST SDG PL) został zaprojektowany, aby wspierać cyfrową transformację publicznych usług w całej Europie. Jest to zbiór modułowych, wielokrotnego użytku, otwartych rozwiązań cyfrowych, które zapewniają kluczowe funkcjonalności umożliwiające interoperacyjność i komunikację między różnymi systemami IT na poziomie transgranicznym.

System korzysta z następujących technologii:

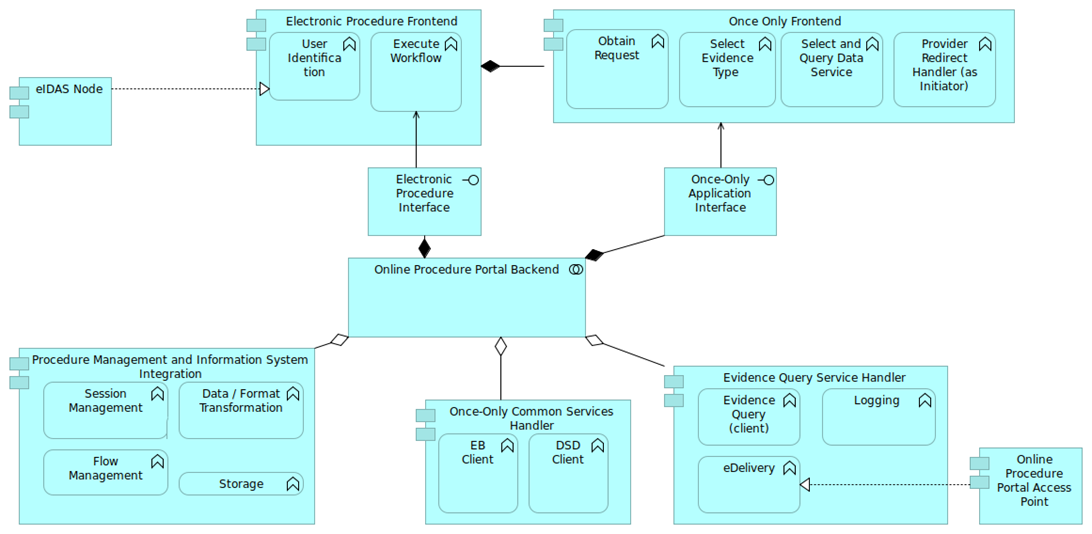
• Java

• Spring (spring boot, spring cloud, freemarker)

• MongoDB

• Angular

Koncepcja obrazująca model logiczny funkcjonowania Systemu Technicznego została zaprezentowana na diagramie poniżej:

Na architekturę ekosystemu Jednolitego Portalu Cyfrowego składają się następujące moduły:

* **PL-Proxy-DostawcaDowodów**

Moduł odpowiedzialny za pobieranie dowodów udostępnianych przez inne kraje UE, w kontekście realizacji e-usług transgranicznych udostępnianych dla podmiotu publicznego z Polski. Zgodnie z modelem integracji opracowanym dla SDG, moduł będzie pełnić rolę OOTS Staging Area Portal. W praktyce będzie realizował następujące funkcje:

• weryfikacja tożsamości osoby pobierającej dowód w ramach Węzła Krajowego,

• zebranie informacji od użytkowników dotyczących szczegółów dowodu jaki ma zostać pobrany, niezbędnych do wskazania rejestru z jakiego będzie on pochodził. Zbieranie tych informacji jest sterowane przy wsparciu modułów KE/UE-OOTS-EvidenceBroker i KE/UE-OOTS-DataServiceDirectory,

• pobranie dowodu z wybranego zagranicznego rejestru,

• zarejestrowanie logów związanych z procesem udostępniania dowodów.

Zakłada się, że moduł może pośredniczyć w pobieraniu dowodów dla wielu e-usług, zarówno dostępnych na Biznes.gov.pl ale także udostępnianych przez inne platformy e-usług administracji publicznej w Polsce.

* **PL-Proxy-RejestrDowodów**

Moduł odpowiedzialny za udostępnianie innym krajom UE dowodów, dla których wystawcą jest podmiot publiczny z Polski. W projekcie SDG planuje się za pomocą tego modułu udostępniać dowody pochodzące z rejestru CEIDG. Zgodnie z modelem integracji opracowanym dla SDG, moduł będzie pełnić rolę OOTS Data Service oraz OOTS Preview Space. W praktyce będzie realizował następujące funkcje:

• weryfikacja tożsamości osoby pobierającej dowód w ramach Węzła Krajowego,

• weryfikacja czy osoba ma prawo do dokumentu dowodu o który wnosi,

• zebranie od użytkownika wymaganych informacji niezbędnych do udostępniania dowodu,

• pobranie dowodu z wybranego rejestru (w przypadku projektu będzie to CEIDG),

• podgląd dowodu dla użytkownika przed jego udostępnieniem do e-usługi transgranicznej w której ma być wykorzystany,

• zebranie zgody od użytkownika na udostępnienie dowodu,

• zarejestrowanie logów związanych z procesem udostępniania dowodów.

Jeżeli dowód będący udostępniany jest dostępny publicznie, jest możliwa rezygnacja z weryfikacji tożsamości osoby pobierającej dowód. Zakłada się, że moduł może pośredniczyć w udostępnianiu dowodów dla wielu rejestrów publicznych w Polsce, nie tylko dla rejestru CEIDG.

* **PL-eDOR-AccessPoint**

Moduł odpowiedzialny za komunikację ramach OOTS modułów PL-Proxy-DostawcaDowodów i PL-Proxy-RejestrDowodów z ich odpowiednikami w innych krajach UE. W praktyce będzie on realizował funkcje operatora e-doręczeń, za pomocą którego będą wymieniane komunikaty i dokumenty

* **Biznes.gov.pl e-usługa transgraniczna**

Jest to e-usługa transgraniczna jaka zostanie zaimplementowana w systemie Biznes.gov.pl z uwzględnieniem transgranicznego pozyskiwania dowodów. E-usługa pozwoli wykonać scenariusz pobierania zaświadczenia pochodzącego bezpośrednio z innego kraju UE za pośrednictwem modułu PL-Proxy-DostawcaDowodów. Zakłada się, że użytkownik e-usługi podczas jej wykonywania, zostanie zapytany czy chce załączyć dowód z innego kraju i jeżeli tak, to zostanie przekierowany do modułu który już dalej poprowadzi użytkownika w celu pozyskania tego dowodu. Po wyrażeniu zgody przez użytkownika na przekazanie dowodu, dokument zostanie przekazany zwrotnie do e-usługi i użytkownik będzie kontynuował realizację e-usługi.

* **Biznes.gov.pl IdP**

Moduł Biznes.gov.pl służy do uwierzytelniania się w ramach tego serwisu. Aby uruchomić e-usługę transgraniczną wymaganie jest logowanie jednak na tym etapie nie jest konieczne logowanie poprzez Węzeł Krajowy gdyż nie ma pewności czy użytkownik skorzysta z możliwości pobierania danych z rejestrów UE.

* **CEIDG**

Rejestr CEIDG jest systemem który m.in. przechowuje dane dotyczące wpisu przedsiębiorców w ramach jednoosobowej działalności gospodarczej oraz wystawia zaświadczenia w tym zakresie. Większość danych wpisowych w CEIDG jest dostępna publicznie ale pewien zakres danych jest niejawny i może być udostępniony wyłącznie po weryfikacji tożsamości i uprawnień osoby która zgłasza zapytanie w tym zakresie. Funkcja udostępniania zaświadczeń o wpisie jest realizowana w sposób automatyczny i istnieje obecnie API które realizuje te funkcje. Ocenia się, że w projekcie SDG może być potrzeba rozbudowy istniejącego API w następujących sytuacjach:

• konieczność wystawiania potwierdzeń w specyficznym formacie,

• konieczność wystawiania różnych potwierdzeń o ograniczonym zakresie informacyjnym w zależności od rodzaju dowodu jaki będzie wystawiany,

• weryfikacji tożsamości osób zalogowanych w trybie transgranicznym (np. przy wykorzystaniu dostawcy tożsamości pochodzącego z poza Polski).

* **PL-WK**

Jest to moduł jaki obecnie istnieje pod adresem Login.gov.pl i dostarcza już możliwości logowania przy wykorzystaniu dostawcy tożsamości z innych krajów. Pełni on rolę Węzła Krajowego oraz Węzła Transgranicznego. Na chwilę obecną lista krajów z którymi działa Węzeł Transgraniczny nie jest pełna i nie zawiera wszystkich krajów UE. Ocenia się, że w projekcie SDG może być potrzeba rozbudowy modułu w następujących sytuacjach:

• konieczność poszerzenia listy krajów UE z którymi Login.gov.pl jest zintegrowany,

• konieczność dodania funkcjonalności umożliwiającej ograniczanie listy dostępnych środków tożsamości przy zalogowaniu na Login.gov.pl do listy środków notyfikowanych w UE.

* **KE/UE-OOTS-DataServiceDirectory**

Moduł przechowuje informacje na temat lokalizacji właściwych serwisów UE-OOTS-DataService jakie są w stanie udostępnić dowody wskazane przez użytkownika e-usługi transgranicznej. W architekturze przewidziano dla każdego z krajów UE możliwość skorzystania z gotowego modułu utrzymywanego przez KE oraz także udostępnienie jednego takiego modułu indywidualnie przez dany kraj UE. Niezależnie od sposobu w jaki jest realizowana funkcjonalność tego modułu, każdy z krajów UE jest odpowiedzialny za zarządzania i utrzymywanie w aktualności wpisów w tym module (w zakresie swojego kraju). W Polsce sugeruje się skorzystanie z modułu udostępnionego przez KE do którego będzie dostęp poprzez GUI webowe. Istnieje także możliwość dla krajów korzystających z rozwiązania KE aby zarządzać danymi znajdującymi się w tym module przy pomocy API ale na obecnym etapie rozwoju tego rozwiązania wydaje się to zbyteczne. Istnieje przypadek, w którym implementacja tego modułu po stronie Polski będzie konieczna – dotyczy to kwestii wydawania zaświadczeń potwierdzających rejestrację firmy, które byłyby wystawiane przez KRS lub CEIDG w zależności od wartości identyfikatora NIP/REGON. Na tym etapie analizy zakłada się jednak rozdzielanie tych zaświadczeń według rodzaju rejestru który jest właściwy do ich wystawiania, więc nie będzie potrzeby wskazywania w tym module mapowania identyfikatora na rodzaj rejestru dla każdej pozycji w bazie firm.

* **KE/UE-OOTS-EvidenceBroker**

Moduł będący w odpowiedzialności KE lub innych krajów UE.

Moduł przechowuje informacje na temat rodzajów dowodów wystawianych w danym kraju, w kontekście ustandaryzowanej listy wymagań jakie są niezbędne do spełnienia w celu zrealizowania e-usługi transgranicznej. Do każdego dowodu można także przypisać zestaw dodatkowych atrybutów, które są niezbędne do jednoznacznego określenia rejestru przechowującego wymagany dowód. Przykładem takiego atrybutu może być lokalizacja w przypadku gdy mamy do czynienia z rejestrami lokalnymi.

W architekturze przewidziano dla każdego z krajów UE możliwość skorzystania z gotowego modułu utrzymywanego przez KE oraz także udostępnienie jednego takiego modułu indywidualnie przez dany kraj UE. Niezależnie od sposobu w jaki jest realizowana funkcjonalność tego modułu, każdy z krajów UE jest odpowiedzialny za zarządzania i utrzymywanie w aktualności wpisów w tym module (w zakresie swojego kraju).

* **UE-eDOR-AccessPoint**

Moduł będący w odpowiedzialności innych krajów UE

Moduł odpowiedzialny za komunikację ramach OOTS dla modułów udostępnianych przez inne kraje UE. W praktyce będzie on realizował funkcje operatora e-doręczeń, za pomocą którego będą wymieniane komunikaty i dokumenty.

* **UE-OOTS-ProcedurePortal**

Moduł będący w odpowiedzialności innych krajów UE

Moduł odpowiedzialny za udostępnianie e-usług transgranicznych, które korzystają z możliwości pobierania dowodów udostępnianych przez inne kraje UE. W ramach jednego kraju UE, może być wiele takich modułów.

* **UE-OOTS-DataService**

Moduł będący w odpowiedzialności innych krajów UE

Moduł odpowiedzialny za udostępnianie dowodów dla e-usług transgranicznych, udostępniany przez inne kraje UE. W ramach jednego kraju UE, może być jeden lub wiele takich modułów. Na diagramie w ramach tego modułu zakłada się realizację dwóch ról przewidzianych w architekturze integracji OOTS – czyli Data Service i Preview Space. W praktyce implementacja w poszczególnych krajach UE może przewidywać rozdzielenie tych modułów na osobne komponenty jednak z punktu widzenia integracji w projekcie SDGPL i opracowywanej koncepcji funkcjonowania Systemu Technicznego nie ma to żadnego znaczenia.

* **UE-WK**

Moduł będący w odpowiedzialności innych krajów UE

Jest to moduł jaki dostarcza możliwości logowania przy wykorzystaniu dostawcy tożsamości jakie udostępniają inne kraje UE. Jest to odpowiednik modułu Login.gov.pl jaki kraje UE są zobowiązane do wdrożenia i utrzymywania.

Poniżej znajduje się wykaz aplikacji ST SDG PL wraz z ich opisem:

|  |  |
| --- | --- |
| Keycloak | IDP, integracja z WK i WT |
| api-gateway | gateway służący do komunikacji backend-frontend, zawiera reguły routes wystawionych na zewnątrz endpointów |
| ceidg-api-client | klient dla API CEIDG, odpytuje i pobiera dokumenty z CEIDG |
| conversation-manager | przechowuje dane sesji użytkowników, parametry wywołania oraz wysłane requesty |
| domibus-client | klient Domibus, odbiera i obsługuje oraz konstruuje i wysyła wiadomości z Domibusa |
| evidence-provider | mikroserwis obsługujący ścieżkę providera dla dokumentów ewidencji, zawiera endpointy dla aplikacji frontendowej strony dostarczającej ewidencje |
| evidence-repository | repozytorium dokumentów w Mongo, przechowuje i zwraca odebrane z innych krajów dokumenty ewidencji |
| evidence-requester | mikroserwis obsługujący ścieżkę requestera dla dokumentów ewidencji, zawiera endpointy dla aplikacji frontendowej requestującej o ewidencje |
| frontend | aplikacja frontendowa dla użytkownika, formularz budowania parametrów wysyłki wiadomości |
| oots-common-services-client | klient serwisów DSD (Data Service Directory) i EB (Evidence Broker), odpytuje API tych serwisów |
| oots-validation-service | walidowanie wiadomości, zawiera schematrony potrzebne do walidacji |
| Baza Mongo |  |

Przyjmuje się, że System Techniczny Jednolitego Portalu Cyfrowego musi spełniać następujące minimalne wymagania:

* 1. Wymagania Aplikacji:

Aplikacja + baza: 11vCPU, 18GB RAM, 50GB dysk

* 1. Wymagania dla klastra:

Kubernetes (RKE2) + komponenty (100GB/node dysk)

W czasie audytu nie przewiduje się udostępniania poprzez ST SDG PL obsługi krajowych usług innych niż z systemu Biznes.gov.pl.

Planuje się wykonanie dwóch faz audytu w trakcie realizacji umowy, przy czym zakres prac w ramach obu faz będzie zbliżony. W ramach 2 fazy audytu Wykonawca zobowiązany będzie dodatkowo do zweryfikowania usunięcia ewentualnych podatności zidentyfikowanych w ramach 1 fazy.

1. Platforma Elektronicznego Fakturowania, Książka Adresowa PEF i Portal efaktura.gov.pl

*Aplikacja Brokera PEF*

Aplikacja Brokera PEF służy użytkownikom do wymiany elektronicznych dokumentów, w tym ustrukturyzowanych faktur elektronicznych. Wykonawca wykona audyt aplikacji i systemu Brokera PEF.

Audytem zostanie objęte nie więcej niż 15 serwerów fizycznych/wirtualnych (jeden portal internetowy). Audytem objęte zostanie nie więcej niż 20 formularzy HTML oraz nie więcej niż 2 zapory sieciowe. Audytem powinno być objęte nie więcej niż 10 przełączników, nie więcej niż 2 load-balancery oraz nie więcej niż 2 routery (trasowniki). Zakres audytu obejmuje nie więcej niż 5 dedykowanych systemów bezpieczeństwa – typy minimum IDS/IPS, UTM, WAF. Dodatkowo, podmiot utrzymujący system PEF zapewnia usługi SOC. System posiada nie więcej niż 5 hostów w puli adresacji zewnętrznej.

Aplikacja zawiera około 40 podstron i ekranów, z czego około połowa to formularze dynamicznie generowane. Łączna liczba pól w formularzach przekracza 300, a liczba wszystkich używanych zmiennych w systemie przekracza 1000.

Aplikacja PEF umożliwia utworzenie różnych typów użytkowników, w tym przede wszystkim: a) standardowego użytkownika o różnym poziomie uprawnień, ale bez uprawnień administratorskich, b) super użytkownika danego konta podmiotu o poziomie uprawnień administratora, c) zarządcy – konta administrowania systemem ze strony MRiT.

*Portal efaktura.gov.pl i Książka Adresowa PEF*

Portal efaktura.gov.pl stanowi kompendium wiedzy o elektronicznym fakturowaniu w zamówieniach publicznych oraz repozytorium dokumentacji użytkowników. Portal umożliwia wyszukanie adresu PEF odbiorcy dokumentu, przechowywanego w bazie adresowej podmiotów zarejestrowanych na PEF – Książce Adresowej PEF.

Audytem zostanie objęte:

− nie więcej niż 6 serwerów fizycznych/wirtualnych

− portal internetowy oraz aplikacja webowa

− nie więcej niż 18 formularzy HTML

− nie więcej niż 2 zapory sieciowe działające w trybie HA

− 1 load-balancer, 2 przełączniki i 2 trasowniki działające w trybie HA

− dla każdego z systemów zakres audytu obejmuje nie więcej niż 5 dedykowanych systemów bezpieczeństwa – typy minimum IDS/IPS, UTM, WAF.

Serwerownie systemów PEF znajdują się na terenie województwa śląskiego, przy czym Zamawiający dopuszcza wykonywanie prac zdalnie pod warunkiem uzgodnienia szczegółów dotyczących audytu z podmiotem świadczącym usługi utrzymania ww. systemów.

1. Platforma Internetowa Polityki Zakupowej Państwa

Platforma stanowić będzie centralne źródło wiedzy z zakresu zamówień publicznych. Dzięki niej kompleksowa i darmowa wiedza o zamówieniach publicznych będzie łatwo i szybko dostępna zarówno dla zainteresowanych wykonawców, w tym z sektora MŚP, jak i dla wszystkich innych praktyków zamówień publicznych. Obecnie udostępniane są podstawowe funkcjonalności systemu, przy czym nie będą one stanowiły przedmiotu potencjalnych prac audytowych.

W ramach audytu Zamawiający może powierzyć wykonawcy realizację prac związanych z badaniem dodatkowych modułów funkcjonalnych Platformy:

1. Moduł e-learning: znajdą się na nim szkolenia w formie e-learning, obejmujące najważniejsze elementy z obszaru zamówień publicznych. Dzięki temu uczestnicy będą mogli pogłębić swoją wiedzę i umiejętności - w elastyczny sposób i w dogodnym dla siebie czasie.
2. Moduł webinarium: zapewni możliwość organizowania i prowadzenia warsztatów i szkoleń online z obszaru zamówień publicznych. Na szkoleniach tych wykładowcy i eksperci będą mogli dzielić się wiedzą i doświadczeniem z wykonawcami oraz przedsiębiorcami. Dzięki temu dostęp do wiedzy będzie łatwiejszy i wygodniejszy.
3. Moduł certyfikacja: po wejściu w życie przepisów o certyfikacji wykonawców zamówień publicznych zapewniony zostanie dostęp do wydanych certyfikatów, co ułatwi przedsiębiorcom posługiwanie się nimi. Przedsiębiorca nie będzie bowiem musiał składać certyfikatu zamawiającemu, gdyż zamawiający będzie mógł samodzielnie pobrać certyfikat z bazy.

System zostanie zaimplementowany w oparciu i z wykorzystaniem komponentów oprogramowania posiadających otwarte tryby licencjonowania (Open Source).

Na potrzeby wszystkich maszyn wirtualnych wykorzystanie zostanie system operacyjny Ubuntu 22.04 LTS. Warstwa prezentacji (frontend) zrealizowana zostanie w postaci aplikacji internetowej w technologii React oraz Bootstrap. Warstwa logiki (backend) zrealizowana zostanie w postaci API w technologii .NET oraz języku C#. Warstwa danych (DB) zrealizowana zostanie w postaci relacyjnej bazy danych PostgreSQL oraz silnika wyszukiwania ElasticSearch. Za zarządzanie procesami biznesowymi odpowiadać będzie silnik procesowy Camunda Zeebe. Silnik ten będzie realizował procesy biznesowe zidentyfikowane w ramach prac analitycznych. Monitorowanie wewnętrzne zrealizowane zostanie za pośrednictwem oprogramowania Grafana i InfluxDB. Ruch sieciowy obsługiwany będzie przez HAProxy. Kontenery aplikacji obsługiwać będzie DockerServer. W celu wysyłki wiadomości z Systemu wykorzystany zostanie serwer pocztowy Postfix.

W celu optymalizacji zasobów wszystkie serwery zarówno te podstawowe jak i zapasowy będą działać na równych zasadach – wszystkie będą równie obciążane i na każdym z serwerów będzie pewien zapas mocy pozwalający na przejście maszyn na wypadek awarii. Wszystkie serwery pracujące w ramach platformy będą połączone z macierzą dyskową, na której przetrzymywane będą wszystkie informacje związane z maszynami wirtualnymi dzięki czemu możliwe będzie migrowanie w locie maszyn między węzłami klastra wirtualizacyjnego. Do całego rozwiązania dostęp będzie chroniony na poziomie sieciowym dzięki zastosowaniu urządzenia UTM lub WAF, na takim urządzeniu będzie też terminowany ruch SSL.

System jest zbudowany zgodnie z SOA (Service Oriented Architecture) w oparciu o niezależne moduły, z których każdy realizuje zestaw określonych funkcji i jest udostępniany użytkownikom jako usługa.

Moduł administracyjny jest dostępny z wyznaczonych lokalizacji, nie ma do niego publicznego dostępu.

System zintegrowany jest z Systemami zewnętrznymi takimi jak Węzeł Krajowy, API BZP, API UZP, API TED, eKONTROLE, Hurtownią Danych CEIDG. Komunikacja na stykach integracyjnych jest w pełni szyfrowana, całość transmisji pomiędzy Systemami odbywa się w szyfrowanym kanale komunikacyjnym SSL. Komunikacja odbywa się za pośrednictwem API lub za pośrednictwem żądań HTTP-POST.

**Szczegółowa dokumentacja poszczególnych systemów, o których mowa w pkt. a) – c) może zostać udostępniona do wglądu w siedzibie Zamawiającego w terminie pomiędzy publikacją ogłoszenia a terminem składania ofert, po uprzednim złożeniu przez wnioskującego Wykonawcę oświadczenia o zachowaniu poufności.**

1. Opis i zakres czynności audytowych

Przewiduje się realizację poszczególnych czynności na nie więcej niż dwóch, wskazanych przez Zamawiającego środowiskach danego systemu

Poniższa tabela prezentuje maksymalny wysokopoziomowy zakres prac audytowych w odniesieniu do danego systemu:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Czynność | ST SDG PL | Systemy PEF | Platforma Internetowa Pzp (prawo opcji – wybrane czynności) | Inne  (prawo opcji – wybrane czynności) |
| Testy bezpieczeństwa / testy penetracyjne | X | X | X | X |
| Analiza zagrożeń i podatności | X | X | X | X |
| Analiza kodu źródłowego | X |  | X |  |
| Audyt bezpieczeństwa przetwarzania danych i ochrony danych | X | X | X |  |
| Analiza architektury sieciowej | X | X |  | X |
| Analiza bezpieczeństwa konfiguracji urządzeń i aplikacji | X | X | X | X |
| Analiza funkcjonowania systemów bezpieczeństwa | X | X |  |  |
| Audyt wydajności | X |  | X | X |

Szczegółowy zakres danych czynności audytowych zostanie ustalony na etapie zlecenia danego zadania lub zlecenia w ramach prawa opcji.

1. Testy bezpieczeństwa / testy penetracyjne

Czynność polega na przeprowadzeniu testów penetracyjnych i symulowanych ataków (wg najnowszych wytycznych OWASP wymienionych na liście TOP10 aktualnej na dzień realizacji audytu) obejmujących:

* testy bezpieczeństwa aplikacji pod kątem, m.in.:

- ataków semantycznych na adres URL,

* 1. - ataków związanych z ładowaniem plików,
  2. - ataków typu Cross-Site Scripting,
  3. - ataków typu Cross-Site Request Forgery,
  4. - ataków typu MITM (Man in the Middle),
  5. - ataków typu Cross Site Tracing,
  6. - ataków typu Session Hijacking / Session Fixation,
  7. - ataków typu Forced Browsing,
  8. - ujawnienia kodu/ścieżki dostępu (Path Disclousure),
  9. - ujawnienia parametrów ograniczających (Parameter Delimiter)
  10. - podrabiania zarządzania formularza,
  11. - sfałszowania żądania http,
  12. - ujawnienia danych przechowywanych w bazie,
  13. - trawersowania katalogów (Path Traversal),
  14. - ujawniania kodu źródłowego,
  15. - przepełnienia bufora lub stosu,
  16. - wstrzykiwania kodu wykonywalnego innych języków programowania (np. SQL Injection / JSON Injection),
  17. - niepożądanego przekierowania,
  + badania enumeracji i wykorzystania znanych podatności w celu uzyskania nieautoryzowanego dostępu,
  + badania możliwości podszywania się pod użytkowników i uzyskania nieautoryzowanego dostępu do systemu
  + badania możliwości podszywania się pod użytkowników uprzywilejowanych i uzyskania dostępu do systemu
  + badania możliwości zablokowania dostępu do systemu wszystkim lub wybranym użytkownikom,
  + badania możliwości usunięcia lub modyfikacji danych w systemie.

1. Analiza zagrożeń i podatności

Czynność polega na:

* Analizie wdrożeń rozwiązań informatycznych obszaru monitorowania bezpieczeństwa IT,
* Detekcji błędów aplikacyjnych,
* Recenzji architektury logicznej,
* Analizie podatności w zainstalowanej wersji serwera,
* Skanowaniu podatności w udostępnionych usługach sieciowych,
* Detekcji podatności w udostępnionych aplikacjach webowych.

1. Analiza kodu źródłowego

Czynność polega na analizie wskazanego przez Zamawiającego kodu źródłowego lub jego wycinka celem zidentyfikowania:

* Niewspieranych lub niebezpiecznych bibliotek,
* Naruszeń licencyjnych,
* Nieprawidłowo działającej architektury,
* Zagrożeń bezpieczeństwa wynikających z zastosowanego kodu.

1. Audyt bezpieczeństwa przetwarzania danych i ochrony danych

Czynność polega na przeprowadzeniu audytu bezpieczeństwa przetwarzania danych zgodnie z wymaganiami wymienionymi w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności oraz zgodnie z normami: ISO 27001 „Technika informatyczna. Techniki Bezpieczeństwa. systemu zarządzania bezpieczeństwem informacji. Wymagania” i ISO 27002 „Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji”.

W audytowanych systemach nie będą przetwarzane dane niejawne w rozumieniu ustawy o ochronie informacji niejawnych z 5 sierpnia 2010 (Dz. U. z 2010 r. nr 182, poz. 1228).

W obszarze zapewnienia bezpieczeństwa przetwarzanych danych oraz ochrony danych, audytowane systemy powinny zagwarantować:

a. poufność – zabezpieczenie danych przed ich udostępnieniem nieuprawnionemu odbiorcy,

b. integralność – zabezpieczenie danych przed modyfikacją lub zniekształceniem przez nieuprawnionych użytkowników,

c. rozliczalność – określenie i weryfikowanie odpowiedzialności za wykorzystanie systemu,

d. autentyczność – weryfikacje tożsamości podmiotów i prawdziwości zasobów,

e. niezawodność – gwarancja oczekiwanego zachowania systemu.

Audyt obejmuje sprawdzenie aktualnego stanu przetwarzania danych osobowych zarówno pod kątem zagadnień technicznych, organizacyjnych oraz prawnych ze szczególnym uwzględnieniem wymagań opisanych w ustawie o ochronie danych osobowych.

Maksymalny zakres czynności audytowych:

a. Przegląd i analiza dokumentacji, w tym analiza dokumentacji polityk bezpieczeństwa i procedur, pod kątem zgodności z wymaganiami (w zakresie jak wyżej) Rozporządzenia, ze szczególnym uwzględnieniem zagadnień IT.

b. Weryfikacja zgodności systemów z wymaganiami Rozporządzenia (w zakresie jak wyżej), ze szczególnym uwzględnieniem zagadnień IT.

1. Analiza architektury sieciowej

Czynność obejmuje:

W zakresie architektury sieciowej

- weryfikacja sieci LAN na strefy sieciowe (w tym wykorzystanie urządzeń typu firewall oraz VLAN),

- określenie usług działających w wybranych podsieciach (do 10 podsieci – nie więcej niż 15 hostów dla jednego systemu),

- poszukiwanie podatności w wybranych podsieciach (do 10 podsieci – nie więcej niż 15 hostów dla jednego systemu),

- weryfikacja mechanizmów ochronnych w warstwie 2 i 3 modelu OSI,

- weryfikacja dostępu do Internetu z LAN,

- szczegółowa analiza komunikacji sieciowej,

- weryfikacja zasad utrzymania sieci,

- analiza wersji oprogramowania pod kątem znanych podatności (firmware),

- analiza konfiguracji dostępu do urządzenia,

- przegląd konfiguracji dot. użytkowników korzystających z urządzenia, praw dostępu, list dostępów, testy słabych haseł,

- analiza konfiguracji i reguł VPN,

- analiza wykorzystanych mechanizmów kryptograficznych,

- analiza zasad filtracji ruchu sieciowego,

- analiza pod kątem obecności niepożądanych usług,

- analiza mechanizmów logowania zdarzeń

W zakresie brzegu sieci:

- weryfikacja topologii/architektury sieci,

- testy szczelności systemów klasy firewall (w tym działania funkcji IPS obsługującej w czasie rzeczywistym zagrożenia typu nadużycie protokołu, próby tunelowania, oprogramowania typu exploit, kontrola aplikacji, ataki ogólnego typu bez predefiniowanych sygnatur, ruchu generowanego przez szkodliwe oprogramowanie, podatności serwera i klienta wraz z możliwością definiowania własnych sygnatur, regularności aktualizacji firewall w celu przeciwdziałania nowym zagrożeniom, itp.)

- ogólna analiza komunikacji sieciowej z poziomu sieci Internet,

- skanowanie portów różnymi technikami, w celu wykrycia potencjalnych luk bezpieczeństwa w udostępnianych usługach,

- wykrywanie usług sieciowych udostępnionych w sieci Internet,

- próba detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniach dostępnych z sieci Internet,

- testowanie odporności usług wystawionych do sieci Internet na ataki „Denial of Service” co najmniej 2 metodami zaproponowanymi przez Wykonawcę,

- testowanie odporności usług wystawionych do sieci Internet, za pomocą narzędzi eksploatujących typowe luki bezpieczeństwa.

1. Analiza bezpieczeństwa konfiguracji urządzeń i aplikacji

Czynność polega na:

analizie zgodności konfiguracji i sposobu funkcjonowania urządzeń w tym przede wszystkim:

- weryfikacja udostępnionych usług sieciowych,

- weryfikacja zbędnych usług wraz ze wskazaniem ich podatności,

- weryfikacja zaimplementowanych systemów aktualizacji,

- weryfikacja zaimplementowanych systemów logowania zdarzeń,

- weryfikacja mechanizmów administracji zdalnej,

- weryfikacja przypisania użytkowników do właściwych grup,

- weryfikacja uprawnień zgodnie z pryncypium jak najmniejszych uprawnień (ang. „least privilige”),

- przeprowadzenie prób obejścia uprawnień i uzyskania nieautoryzowanego dostępu do informacji,

- weryfikacja sposobu udostępniania baz danych na poziomie sieciowym,

- analiza implementacji podstawowych zasad hardeningowych bazy danych (np. wyłączenie nieużywanych usług, wyłączenie nieużywanych metod dostępu, konfiguracja uprawnień do obiektów, logowanie zdarzeń, składowanie logów, monitorowanie dostępu do obiektów, monitorowanie instrukcji języka SQL),

- analiza architektury baz danych (np. wykorzystanie mechanizmów autoryzacji oraz uwierzytelniania, segmentacja uprawnień, wykorzystywanie widoków, wykorzystywanie procedur składowych, przechowywanie oraz dostęp do danych wrażliwych, przechowywanie oraz dostęp do danych audytowych, szyfrowanie danych),

- analiza komunikacji z klientami bazodanowymi (mechanizmy kryptograficzne, transfery danych),

- analiza używanych technologii.

Analizie podatności aplikacji:

- wytypowanie wrażliwych punktów w aplikacji,

- inspekcja mechanizmów uwierzytelniania / autoryzacji,

- zabezpieczenia interfejsu użytkownika za pomocą captcha oraz za pomocą zweryfikowanego certyfikatu, two-factor authentication (2FA)

- weryfikacja implementacji mechanizmów ochronnych dla serwerów aplikacyjnych,

- weryfikacja obsługi błędów,

- analiza poziomu bezpieczeństwa oferowanego przez aplikacje.

1. Analiza funkcjonowania systemów bezpieczeństwa

Czynność polega na:

analizie i ocenie funkcjonowania następujących systemów bezpieczeństwa:

- System antywirusowy.

- System antyspamowy.

- System DLP (Data Leak Prevention/Data Loss Prevention).

- System Firewall.

- System backupowy wraz z testem odtworzenia systemu z backupu (Zamawiający nie wymaga odtwarzania systemu na zasobach Wykonawcy), ocena lokalizacji baz danych zawierających kopie bezpieczeństwa (bezpieczeństwo ośrodka, ośrodek zapasowy).

- System zasilania awaryjnego.

1. Audyt wydajności

Czynność obejmuje testy serwera www: dla jednoczesnych sesji: 0…5000 (maksymalnie) – pomiar czasów odpowiedzi serwera i czasu załadowania strony. Czasy odpowiedzi i ładowania maja obejmować wartości średnie i maksymalne dla każdego punktu pomiarowego.

1. Zakres prac realizowanych w ramach prawa opcji

Zamawiający ma prawo do skorzystania z prawa opcji w postaci zleceń wskazujących zakres wykonywanych czynności audytowych w odniesieniu do zadań określonych w rozdz. I pkt. 4-5 OPZ. Zakres zlecanych czynności nie będzie wykraczał ponad zdefiniowane w pkt a) – h) powyżej. Ponadto, w ramach prawa opcji mogą być zlecane retesty wcześniejszych działań audytowych. Czasochłonność danego zlecenia będzie wyceniana przez Wykonawcę każdorazowo po wskazaniu przez Zamawiającego zakresu tego zlecenia i będzie podlegała akceptacji Zamawiającego.

Łączna liczba roboczogodzin przeznaczonych na realizację prawa opcji nie może przekroczyć 400.

1. Opis procesu realizacji zadań i wyniki prac
2. Zadania audytowe

Dotyczy zadań opisanych w rozdz. I pkt 1-3.

Orientacyjny harmonogram realizacji poszczególnych zadań znajduje się w rozdz. V, przy czym terminy te mogą ulec zmianie. Zlecenie będzie zawierać m. in. proponowaną datę rozpoczęcia i zakończenia czynności oraz obszar podlegający audytowi/testom.

Wykonawca uwzględniając wymagania oraz informacje zawarte w zleceniu, w terminie 14 dni liczonych od dnia otrzymania zlecenia, przedstawi Zamawiającemu szczegółową propozycję Planu audytu/testów wydajności. Zamawiający po otrzymaniu propozycji planu, w terminie 7 dni liczonych od dnia jej otrzymania, przedstawi Wykonawcy ewentualne uwagi do planu, bądź dokona jego zatwierdzenia. W przypadku zgłoszenia uwag, zamawiający wskaże termin (nie krótszy, niż 3 dni robocze) przedstawienia przez Wykonawcę poprawionego planu. Następnie jeśli Wykonawca przedstawi poprawiony plan, Zamawiający w terminie 7 dni kalendarzowych może dokonać zatwierdzenia go, a jeśli poprzednio zgłoszone uwagi nie zostały w pełni uwzględnione przez Wykonawcę, wtedy Zamawiający może ponownie zgłosić uwagi. Wykonawca przystąpi do wykonywania audytu/testów nie wcześniej niż w dniu zatwierdzenia planu.

Czynności audytowe/testowe dla danego zadania nie mogą trwać dłużej niż 45 dni kalendarzowych. Po zakończeniu realizacji zadania, w terminie nie dłuższym niż 7 dni kalendarzowych liczonych od jego zakończenia, Wykonawca przedstawi Zamawiającemu Raport z wykonanego zadania. Zamawiający w terminie 7 dni kalendarzowych liczonych od dnia otrzymania raportu, przedstawi Wykonawcy ewentualne uwagi do wykonanych prac, bądź dokona zatwierdzenia raportu. W przypadku zgłoszenia uwag do raportu, zamawiający wskaże termin (nie krótszy, niż 3 dni robocze) na prawidłowe wykonanie raportu. W przypadku raportu, co do którego zostały zgłoszone uwagi, Zamawiający w terminie 7 dni kalendarzowych dokona zatwierdzenia poprawionego przez Wykonawcę raportu, a jeśli poprzednio zgłoszone uwagi nie zostały uwzględnione przez Wykonawcę, wtedy Zamawiający może ponownie zgłosić uwagi.

Rozliczeniu podlegają wyłącznie zadania zatwierdzone przez Zamawiającego.

1. Zlecenia w ramach prawa opcji

Dotyczy zadań opisanych w rozdz. I pkt. 4-5.

Zamawiający wystawi Zlecenie na realizację zadania lub części zadania, które będzie zawierać m. in. proponowaną datę rozpoczęcia i zakończenia prac oraz zakres prac. Zadania te będą rozliczane w ramach puli roboczogodzin przysługujących do wykorzystania w ramach umowy, przy czym realizacja danego zadania lub jego części nie może prowadzić do przekroczenia tej puli.

Wykonawca uwzględniając wymagania oraz informacje zawarte w zleceniu w terminie 7 dni liczonych od daty otrzymania zlecenia przedstawi Zamawiającemu Propozycję realizacji zadania (lub jego części) wraz ze wskazaniem pracochłonności (wyrażonej w roboczogodzinach) potrzebnej na jego wykonanie. Zamawiający po otrzymaniu propozycji, w terminie 7 dni kalendarzowych liczonych od dnia jej otrzymania, przedstawi Wykonawcy ewentualne uwagi do propozycji, bądź dokona jej zatwierdzenia. W przypadku zgłoszenia uwag Zamawiający wskaże termin, nie krótszy niż 3 dni robocze, na przedstawienie przez Wykonawcę poprawionej propozycji realizacji zlecenia. Następnie jeśli Wykonawca przedstawi poprawioną propozycję realizacji zlecenia, Zamawiający w terminie 7 dni kalendarzowych może dokonać zatwierdzenia jej, a jeśli poprzednio zgłoszone uwagi nie zostały w pełni uwzględnione przez Wykonawcę, wtedy Zamawiający może ponownie zgłosić uwagi z terminem. Wykonawca przystąpi do wykonania prac na podstawie propozycji zatwierdzonej przez Zamawiającego.

Proponowany termin wykonania prac zostanie określony w zleceniu przez Zamawiającego. Faktyczny termin realizacji zostanie wskazany przez Wykonawcę w Propozycji realizacji zlecenia, przy czym termin ten nie może być dłuższy niż 30 dni kalendarzowych. Wykonawca najpóźniej w ostatnim dniu realizacji danego zlecenia Wykonawca przedstawi Zamawiającemu Zamawiający w terminie 7 dni liczonych od dnia otrzymania raportu, przedstawi Wykonawcy ewentualne uwagi do wykonanych prac, bądź dokona zatwierdzenia raportu. W przypadku zgłoszenia uwag do raportu, zamawiający wskaże termin (nie krótszy, niż 3 dni robocze) na prawidłowe wykonanie raportu. W przypadku raportu, co do którego zostały zgłoszone uwagi, Zamawiający w terminie 7 dni kalendarzowych dokona zatwierdzenia poprawionego przez Wykonawcę raportu, a jeśli poprzednio zgłoszone uwagi nie zostały uwzględnione przez Wykonawcę, wtedy Zamawiający może ponownie zgłosić uwagi Raport z wykonanego zlecenia.

Rozliczeniu podlegają wyłącznie zlecenia, których realizacja została zatwierdzona przez Zamawiającego. Zamawiający będzie realizował płatności za wykonane zlecenia każdorazowo po ich wykonaniu. Podstawę stanowić będą zatwierdzone raporty. Zamawiający ma prawo do rezygnacji z realizacji danego zlecenia w dowolnym momencie przed jego zatwierdzeniem, bez podania przyczyny.

1. Wymagania dotyczące współpracy Zamawiającego z Wykonawcą

Zamawiający dopuszcza możliwość przeprowadzenia prac audytowych w formie zdalnej. W przypadku konieczności przeprowadzenia audytu stacjonarnego, jego zakres zostanie ustalony z Zamawiającym na etapie realizacji audytu. W takim przypadku Wykonawca uzyska dostęp do infrastruktury w zakresie ustalonym z Zamawiającym.

Serwerownie znajdują się w okolicach Warszawy, Katowic lub innych miejscowości na terenie Polski – Wykonawca musi uwzględniać możliwość wykonywania podróży służbowych w celu realizacji audytu stacjonarnego, w ramach wynagrodzenia, które otrzyma.

Zamawiający nie dopuszcza możliwości włączenia maszyny Wykonawcy do sieci w audytowanej infrastrukturze.

W ramach współpracy Wykonawca i Zamawiający wyznaczają w swoich strukturach osobę prowadzącą zadanie lub zlecenie oraz osobę zastępującą. Wykonawca zobowiązany jest do sprawnej i terminowej realizacji zamówienia oraz stałej współpracy z Zamawiającym, w tym:

- pozostawania w stałym kontakcie (kontakt telefoniczny oraz drogą elektroniczną; spotkania z Zamawiającym w miarę potrzeb; wyznaczenie osoby do kontaktów roboczych);

- informowania o stanie prac, pojawiających się problemach i innych zagadnieniach istotnych dla realizacji badania.

d) Procedura odbiorowa

W terminie 7 dni od dnia zrealizowania danego zadania lub części zadania w ramach zlecenia Wykonawca sporządzi protokół odbioru zadania i przekaże go Zamawiającemu do akceptacji. Protokół powinien być podpisany przez obie Strony lub osoby przez nie upoważnione. Protokół odbioru zadania lub części zadania w ramach zlecenia powinien zawierać w szczególności:

a) dzień i miejsce wystawienia i odbioru zadania,

b) oświadczenie Zamawiającego, o braku lub istnieniu zastrzeżeń lub nieprawidłowości w realizacji zadania,

c) podpisy Stron lub osób upoważnionych.

W razie uchylania się Wykonawcy od sporządzenia protokołu w uzgodnionym terminie, Zamawiający może samodzielnie sporządzić protokół odbioru zadania lub jego części i treść takiego protokołu uznać za zaakceptowaną przez Wykonawcę.

Zadanie w ramach prawa opcji zostaje uznane za zrealizowane w przypadku zakończenia umowy lub wyczerpania puli roboczogodzin przeznaczonych na to zadanie, przy czym Wykonawcy przysługuje z tego tytułu wynagrodzenie wyłącznie w wysokości odpowiadającej liczbie roboczogodzin wynikającej z udzielonych przez Zamawiającego zleceń.

1. Prognozowany harmonogram prac

1. Wykonanie I fazy audytu bezpieczeństwa Systemu Technicznego Jednolitego Portalu Cyfrowego (ST SDG PL) – Q1/Q2 2025 r.

2. Wykonanie II fazy audytu bezpieczeństwa Systemu Technicznego Jednolitego Portalu Cyfrowego (ST SDG PL) po optymalizacji systemu – Q4 2025/Q1 2026 r.

3. Przeprowadzenie audytu bezpieczeństwa systemów teleinformatycznych Platformy Elektronicznego Fakturowania: aplikacji Brokera PEF, Książki Adresowej PEF i Portalu efaktura.gov.pl – Q3/Q4 2025 r.

4. Przeprowadzenie testów cyberbezpieczeństwa i wydajności nowych modułów funkcjonalnych Platformy Internetowej Polityki Zakupowej Państwa – prawo opcji: realizowane w trybie ciągłym, nie później niż 24 miesiące od dnia podpisania umowy.

5. Realizacja doraźnych zleceń wsparcia w zakresie cyberbezpieczeństwa dot. systemów teleinformatycznych MRiT – prawo opcji: realizowane w trybie ciągłym, nie później niż 24 miesiące od dnia podpisania umowy.

1. Załączniki

Szczegółowa dokumentacja audytowanych systemów - załączniki mogą zostać udostępnione do wglądu w siedzibie Zamawiającego po uprzednim złożeniu oświadczenia   
o poufności.