

Załącznik nr 1 do Ogłoszenia o zamówieniu

1. OPIS PRZEDMIOTU ZAMÓWIENIA

1.1. Przedmiotem zamówienia jest wykonanie usługi audytu w zakresie testów bezpieczeństwa systemu eDyplomy - Repozytorium Dyplomów Elektronicznych, dalej zwanej "Usługą".

Według oznaczenia Wspólnego Słownika Zamówień (CPV):

79212000-3- usługi audytu

72800000-8 – usługi audytu komputerowego i testowania komputerów

2. Wstęp

2.1. Niniejszy dokument precyzuje wymagania dotyczące przedmiotu zamówienia poprzez określenie:

- 2.1.1. Celu przedmiotu zamówienia.
- 2.1.2. wymagań w zakresie usług realizowanych w ramach przedmiotu zamówienia,
- 2.1.3. wymagań w zakresie produktów, które mają być wytworzone w związku z realizacją przedmiotu zamówienia,
- 2.1.4. wymagań w zakresie formuły realizacyjnej,
- 2.1.5. usługi/produkty techniczne objęte zamówieniem,
- 2.1.6. miejsca realizacji zamówienia.

3. Cel Usługi

3.1. Usługa zostanie zrealizowana w celu weryfikacji spełnienia przez Zamawiającego wymogów, wynikających z obowiązujących przepisów prawa, nakładających na Zamawiającego obowiązek zapewnienia odpowiedniego systemu zarządzania bezpieczeństwem informacji. W szczególności mają tu zastosowanie przepisy KRI w zakresie, w którym dotyczą one zapewnienia właściwego poziomu bezpieczeństwa w stworzonych usługach/produktach technicznych, tj. par 19 ust. 2 pkt 12 KRI (Dz. U. z 2024 r. poz. 773).

3.2. Główne cele Usługi to:

- 3.2.1. Pozyskanie informacji na temat istniejących podatności i słabości w obszarze bezpieczeństwa audytowanych usług/produktów technicznych.
- 3.2.2. Wiarygodna ocena bezpieczeństwa zasobów usług/produktów technicznych.
- 3.2.3. Rekomendacja rozwiązań w zakresie utrzymania wysokiego poziomu bezpieczeństwa usług/produktów technicznych.

4. Przedmiot zamówienia

- 4.1. Przedmiotem zamówienia jest wykonanie usługi audytu w zakresie testów bezpieczeństwa systemu eDyplomy - Repozytorium Dyplomów Elektronicznych, która powinna obejmować działania podzielone na dwa następujące etapy:

5. Testy bezpieczeństwa (etap I)

- 5.1. W ramach przedmiotu zamówienia Wykonawca powinien przeprowadzić testy bezpieczeństwa polegające na wykonaniu symulacji ataków cybernetycznych nakierunkowanych na zidentyfikowanie podatności przedmiotu zamówienia prowadzone metodą blackbox (bez znajomości kodów źródłowych, ani konfiguracji aplikacji). Usługa powinna obejmować następujący zakres zadań:
 - 5.1.1. wykorzystanie manualnych oraz automatycznych technik ataku,
 - 5.1.2. detekcja błędów aplikacyjnych typu:
- 5.2. Security Misconfiguration (błędy w konfiguracji zabezpieczeń, umożliwiające nieuprawnione działanie);
 - 5.2.1. Sensitive Data Exposure (potencjalna możliwość nieuprawnionego dostępu do wrażliwych danych);
 - 5.2.2. Broken Access Control (błędy w obszarze autoryzacji np. insecure direct object references, authorization bypass);
 - 5.2.3. Using Components with Known Vulnerabilities (użycie komponentów posiadających znane podatności – np. dana wersja komponentu itp);
 - 5.2.4. Injection (SQL injection, noSQL injection, XSS, XXE, Code injection etc.);
 - 5.2.5. Clickjacking ;
 - 5.2.6. CSRF (Cross Site Request Forgery);
 - 5.2.7. Broken authentication and session management (badanie losowości ID sesji, próba detekcji składni parametru sesyjnego, bezpieczeństwa sposobu przesyłania

poświadczeń, weryfikacja, ocena poprawności wygasania sesji);

5.2.8. Code execution (próby wykonania dowolnego kodu na serwerze);

5.2.9. OS Command Injection;

5.2.10. Server-side template injection;

5.2.11. Insecure deserialization;

5.2.12. Server-side request forgery (SSRF);

5.2.13. Insecure communications (np. dostęp do istotnych danych – np. konta administracyjnego bez szyfrowania);

5.2.14. Path traversal;

5.2.15. Open redirection;

5.2.16. Denial of Service (DoS);

5.2.17. File inclusion (local/remote);

5.2.18. File upload vulnerabilities;

5.2.19. HTTP request smuggling;

5.2.20. Business logic vulnerabilities;

5.2.21. JWT attacks;

5.2.22. Race conditions;

5.2.23. Prototype pollution;

5.2.24. Deserialization of untrusted data.

5.3. raport z wykonanych czynności audytowych w ramach etapu I zgodny z zakresem określonym w sekcji **“Wymagania w zakresie dokumentów dostarczonych w związku z wykonanymi usługami”**.

6. Testy bezpieczeństwa (etap II)

6.1. Testy bezpieczeństwa, w ramach których należy sprawdzić poprawność instalacji i konfiguracji usług/produktów technicznych, analiza systemowa stosowanych zabezpieczeń usług/produktów technicznych wykazująca, w szczególności czy zastosowane w ich produkcji technologie są odpowiednie, czy systemy nie są narażone na podatności, czy istnieją nowsze bezpieczniejsze narzędzia w tym zakresie, kontekście najnowszych rozwiązań teleinformatycznych wykorzystywanych w utrzymaniu wysokiego poziomu bezpieczeństwa usług/produktów technicznych, w szczególności chroniących przed zagrożeniami wynikającymi z cyberataków. Usługa w ramach etapu testów kontrolnych musi obejmować następujący zakres zadań:

- 6.1.1. audyt warstwy bazodanowej, w ramach którego wykonane zostaną w szczególności następujące czynności:
- 6.1.2. sprawdzenie wdrożenia podstawowych zasad hardeningowych bazy (np.: dostępność domyślnych użytkowników guest, partycjonowanie bazy, składowanie logów, logowanie nietypowych zdarzeń, dostępność wybranych niebezpiecznych procedur /funkcji składowanych),
- 6.1.3. ogólna recenzja architektury bazy (wykorzystane mechanizmy autoryzacji oraz uwierzytelniania; segmentacja uprawnień, wykorzystanie widoków; wykorzystanie procedur składowanych),
- 6.1.4. identyfikacja i inwentaryzacja:
 - 6.1.4.1. zidentyfikowanie wszystkich instancji baz danych w środowisku;
 - 6.1.4.2. określenie wersji i poziomu aktualizacji silnika bazodanowego;
 - 6.1.4.3. sporządzenie listy usług i portów związanych z bazami danych;
 - 6.1.4.4. sprawdzenie czy wersje poszczególnych komponentów są podatne na znane luki bezpieczeństwa,
- 6.1.5. weryfikacja konfiguracji i uprawnień:
 - 6.1.5.1. przegląd ustawień konfiguracyjnych baz danych pod kątem bezpieczeństwa;
 - 6.1.5.2. analiza uprawnień użytkowników i ról – ocena realizacji zasady najmniejszych uprawnień (least privilege);
 - 6.1.5.3. ocena występowania nieużywanych kont i domyślnych użytkowników;
 - 6.1.5.4. sprawdzenie silnych polityk haseł i mechanizmów uwierzytelniania,
- 6.1.6. testowanie podatności:
 - 6.1.6.1. testy na obecność podatności typu SQL Injection oraz innych typowych ataków na bazę danych;
 - 6.1.6.2. próba wykorzystania domyślnych lub słabych haseł;
 - 6.1.6.3. próby eskalacji uprawnień w ramach bazy danych,
- 6.1.7. szyfrowanie i transmisja danych:
 - 6.1.7.1. weryfikacja stosowania szyfrowania danych w spoczynku (at rest) oraz w transmisji (in transit);
 - 6.1.7.2. sprawdzenie poprawności konfiguracji certyfikatów SSL/TLS i protokołów szyfrujących,
- 6.1.8. kopie zapasowe i odzyskiwanie danych
 - 6.1.8.1. ocena polityki wykonywania kopii zapasowych i procedur odzyskiwania danych;

- 6.1.8.2. Weryfikacja bezpieczeństwa przechowywania backupów (szyfrowanie, dostępność, testy odtwarzania),
- 6.1.9. ograniczanie ekspozycji i segmentacja sieci
 - 6.1.9.1. sprawdzenie czy baza danych nie jest niepotrzebnie wystawiona na zewnątrz (np. publiczny dostęp do portów);
 - 6.1.9.2. ocena segmentacji sieci i konfiguracji firewalli chroniących bazę danych.
- 6.1.10. audyt warstwy sieciowej, w ramach którego wykonane zostaną w szczególności następujące czynności:
 - 6.1.10.1. analiza topologii sieci, ze szczególnym uwzględnieniem urządzeń brzegowych,
 - 6.1.10.2. weryfikacja podziału LAN na strefy sieciowe (w tym wykorzystanie firewalli oraz VLAN/PVLAN),
 - 6.1.10.3. identyfikacja usług działających w sieci LAN wraz z ich wersjami,
 - 6.1.10.4. identyfikacja podatności w oparciu o zidentyfikowane wersje usług.
- 6.1.11. audyt warstwy systemów operacyjnych (serwery, macierze, biblioteki), w ramach którego zostaną wykonane w szczególności następujące czynności:
 - 6.1.11.1. wskazanie zaleceń hardeningowych dla systemu operacyjnego - zwiększających jego bezpieczeństwo,
 - 6.1.11.2. sprawdzenie udostępnionych usług sieciowych,
 - 6.1.11.3. sprawdzenie podziału przestrzeni dyskowej na odpowiednie strefy,
 - 6.1.11.4. sprawdzenie wdrożenia dodatkowych metod ochrony (np.: dodatkowe mechanizmy ochronne zaimplementowane na poziomie kernela, system antywirusowy, itp),
 - 6.1.11.5. sprawdzenie przynależności użytkowników do grup uprzywilejowanych,
 - 6.1.11.6. sprawdzenie uprawnień do najistotniejszych zasobów,
 - 6.1.11.7. sprawdzenie wdrożonego mechanizmu instalacji aktualizacji,
 - 6.1.11.8. sprawdzenie wdrożonego mechanizmu kopii zapasowych,
 - 6.1.11.9. sprawdzenie wdrożonego systemu logowania zdarzeń,
 - 6.1.11.10. sprawdzenie zabezpieczenia systemu w fazie boot,
 - 6.1.11.11. sprawdzenie wykorzystywanego sposobu zarządzania systemem,
 - 6.1.11.12. sprawdzenie kwestii organizacyjnych i proceduralnych: zarządzanie systemem operacyjnym (poziom administratora), prawami dostępu dla użytkowników do plików i katalogów systemu, logowanie zdarzeń i accounting; kopie

zapasowe i odtworzeniowe systemów, awarie i procedury awaryjne, kontrola wewnętrzna. Badanie podatności na ataki (ARP Poisoning, Network Based Testing i Host Based testing), weryfikacja bezpieczeństwa konfiguracji systemu, badanie aktualności oprogramowania systemowego.

6.1.12. weryfikacja ochrony przed szkodliwym oprogramowaniem typu malware i podobne,

6.1.13. raport z wykonanych czynności audytowych w ramach etapu II zgodny z zakresem określonym w sekcji **“Wymagania w zakresie dokumentów dostarczonych w związku z wykonanymi usługami”**.

7. Usługi i produkty techniczne objęte przedmiotem zamówienia - Architektura - główne założenia technologiczne

7.1. Języki programowania – frameworki

7.1.1. Java, framework Spring Boot do tworzenia części backend’owej

7.1.2. Angular – framework do tworzenia frontend’u

7.1.3. SQL – do obsługi zapytań bazodanowych

7.2. Orkiestracja systemu:

7.2.1. Technologia: Kubernetes. Architektura mikroservisowa.

7.3. Bazy danych

7.3.1. Technologia: PostgreSQL w konfiguracji active-pasive

7.3.2. Rodzaje baza danych:

7.3.2.1. Główna - operacyjna – przechowuje dane o dokumentach ich statusy i wszelkie dane operacyjne związane z działaniem systemu

7.3.2.2. Baza na metadane plików z dokumentami otrzymanymi z uczelni (np. surowe dane XML z podpisanym dokumentem), inne pliki (np. wygenerowane PDF z dokumentem), inne dane w postaci surowej zarchiwizowane np. podpisane przez RDE i konserwowane dokumenty itp.

7.3.2.3. Baza audytowa – przechowuje dane i zdarzenia przydatne w audytowaniu pracy systemu

7.3.2.4. Baza obiektów PKI – baza przechowująca dane związane z Infrastrukturą klucza publicznego zawierająca obiekty typu wydane certyfikaty, łańcuchy certyfikatów, listy CRL pobrane z centrów autoryzacyjnych itp.

7.4. Obsługa kolejek zadań i zdarzeń

7.4.1. Technologia: Apache Kafka

7.4.2. Przeznaczenie: obsługa asynchroniczna zadań realizowanych batch'owo oraz obsługa innych zdarzeń np. informacji o potrzebie odświeżenia cache itp.

7.5. Kryptografia

7.5.1. Technologia

7.5.1.1. HSM – urządzenie służące do wykonywania operacji kryptograficznych w tym wykonywania podpisu pieczęcią elektroniczną, spełniające wymogi techniczne:

- 7.5.1.1.1. posiada SDK w postaci provider'a dla Javy w standardzie JSP (Java Security Provider) pozwalający na używanie HSM w kodzie Java z wykorzystaniem funkcji w standardach JCA/JCE (Cryptography Architecture / Java Cryptography Extension)
- 7.5.1.1.2. obsługuje interfejs PKCS11
- 7.5.1.1.3. posiada SDK działające pod kontrolą systemów operacyjnych Windows i Linux
- 7.5.1.1.4. SDK działa zdalnie poprzez sieć i umożliwia wywołanie API HSM'a z wielu klientów równocześnie. HSM powinien działać w klastrze, by zapobiec sytuacji Pojedynczego Punkt Awarii (Single Point Of Failure)
- 7.5.1.1.5. obsługuje klucze asymetryczne RSA oraz ECC a także symetryczne AES oraz certyfikaty X.509
- 7.5.1.1.6. udostępnia poprzez SDK usługi generatora liczb pseudolosowych znajdującego się w HSM. Udostępnienie tych usług dla języka Java powinno być w postaci klasy programistycznej SecureRandom (za pośrednictwem providera)
- 7.5.1.1.7. posiada narzędzie administracyjne pozwalające na wyświetlanie informacji i operacje na: slotach, obiektach w slotach (np. kluczach, certyfikatach), użytkownikach, itp. Może być w postaci narzędzia wołanego z linii komend.
- 7.5.1.2. Rejestrowane dokumenty są w RDE podpisywane pieczęcią kwalifikowaną (klucz prywatny w HSM) oraz znakowane kwalifikowanym czasem (usługa zewnętrzna). Stosowany format Xades z poziomem LTA.
- 7.5.1.3. Dokumenty przysyłane z Instytucji do RDE są podpisywane kwalifikowanym podpisem elektronicznym. Podpis jest walidowany w RDE.

7.6. Przechowywanie plików

7.6.1. Technologia: S3 MinIO

7.6.2. Przeznaczenie: przechowywanie dużej ilości dużych plików (odciąża bazę relacyjną)

w zakresie przechowywania plików)

7.7. Autoryzacja użytkowników:

- 7.7.1. Autoryzacja użytkowników oparta będzie o Moduł Centralnego Logowania (MCL), który oparty jest o Keycloak i stosowany w Systemie POL-on. Stosowany 2gi faktor logowania (2FA oparty np. o Windows Authenticator) oraz do potwierdzania wrażliwych operacji. Użytkownicy mają przyznawane administracyjne role nadające im uprawnienia do poszczególnych funkcjonalności systemu.
- 7.7.2. Autoryzacja obywateli – oparta o Moduł Centralnego Logowania (oparty o Keycloak) oraz Krajowy Węzeł Identyfikacji Elektronicznej.
- 7.7.3. Autoryzacja i kryptografia w API – oparta o SOAP-WSS i wydawane certyfikaty wraz z kluczami w postaci PKCS#12 dla Instytucji mającej prawa do korzystania z API.

7.8. Systemy logowania i monitorowania pracy

- 7.8.1. Technologia: do gromadzenia i przetwarzania logów z pracy systemu zastosowane będą: Graylog, Elasticsearch, Grafana, Monitoring SOC-NOC.

7.9. Powiadomienia oparte o serwer pocztowy System używa różnych bibliotek w wersji OpenSource wspomagających realizację projektu.

7.10. Wielkość kodu (bez open source) to ponad 170 000 linii

7.11. Komponenty logiczne:

- 7.11.1. Aplikacja webowa (Angular) do weryfikacji dokumentów bez potrzeby logowania (około 20 ekranów).
- 7.11.2. Aplikacja webowa (Angular) do przeglądania i pobierania dokumentów. Obywatel uzyskuje dostęp do listy swoich dokumentów za pomocą Krajowego Węzła Identyfikacji Elektronicznej. Aplikacja pozwala na podgląd danych dokumentu oraz pobranie (asynchroniczne zlecenie) podpisanego PDF w formacie PAdES-B-LTA. PDF spełnia też kryteria formatu archiwizacyjnego PDF/A-3U (około 20 ekranów)
- 7.11.3. Aplikacja webowa (Angular) w ramach systemu POL-on pozwalająca pracownikom Instytucji na konfigurację systemu, podgląd i edycje danych, czynności administracyjne itp. (ok 160 zaawansowanych ekranów) . Poszczególne operacje w systemie mogą wykonywać użytkownicy, którym została nadana odpowiednia rola. Role nadawane są w ramach instytucji, która wydaje dokumenty (uczelnie, instytucje naukowe) lub sprawuje nadzór nad procesem wydawania lub weryfikuje dokumenty (ministerstwo, PKA, NAWA, etc.). Uprawnienia w systemie regulowane są systemem ról – około 29 ról, które determinują zakres danych, do których dostęp ma użytkownik oraz rodzaj i liczbę dopuszczalnych dla użytkownika operacji, w tym około

4 ról dla instytucji nadzorujących, typu ministerstwa nadzorujące uczelnie, Polska Komisja Akredytacyjna, Narodowa Agencja wymiany Akademickiej oraz około 25 ról dla instytucji wydających dyplomy.

7.11.4. Aplikacje backendowe w postaci dedykowanych PODów Kubernetesa (kilkanaście rodzajów) służące m.in. do:

7.11.4.1. Zapewnienia usług dla ww. frontendu

7.11.4.2. Dostęp do danych przechowywanych w bazach oraz zasobów przechowujących pliki

7.11.4.3. Batchowe przetwarzanie zadań asynchronicznych

7.11.4.4. Synchronizacja danych z innymi modułami POL-on lub systemami zewnętrznymi

7.12. Obsługa powiadomień

7.13. Dostarczenie usług kryptograficznych

7.14. Łącznie ponad 380 usług/endpointów (na dzień 1.09.2025)

7.15. Aplikacje udostępniające API (SOAP-WSS) dla Instytucji.

7.16. Rozważane jest zastosowanie dodatkowego poolera połączeń między PODami a Postgres np. PGbouncer, PGcat – to poolery połączeń inne niż Hikari który działa w Spring na poziomie pojedynczej aplikacji/PODu (bo to jest dedykowana biblioteka). Zastosowanie poolera może być konieczne, jeśli osiągnięcie większej wydajności będzie wymagać większej ilości POD, a więc i połączeń do bazy (duża ilość połączeń bezpośrednio do bazy degradowe jej wydajność).

8. Wymagania w zakresie dokumentów dostarczonych w związku z wykonanymi usługami

8.1. W wyniku realizacji prac, opisanych w sekcji **“Testy bezpieczeństwa (etap I)”** Wykonawca dostarczy raport, który zawierać będzie:

8.1.1. zakres, metodykę i szczegółowy opis przeprowadzonych prac,

8.1.2. opis przyjętego modelu oceny podatności/zagrożeń,

8.1.3. listę wykrytych podatności i zagrożeń bezpieczeństwa, w tym:

8.1.3.1. szczegółowy opis wykrytych podatności wraz z informacją wskazującą na możliwość wykorzystania i przedstawieniem POC („proof of concept”),

8.1.3.2. klasyfikację stopnia zagrożenia podatności zgodnie z CVSS v3.1,

8.1.3.3. szczegółowe zalecenia ukierunkowane na podniesienie poziomu bezpieczeństwa oraz usunięcie zidentyfikowanych zagrożeń,

8.1.3.4. opis potencjalnych skutków wykorzystania podatności

- 8.1.4. listę dodatkowych zaleceń wynikających z możliwych do zastosowania mechanizmów bezpieczeństwa.
- 8.1.5. informację na temat narzędzi audytowych potrzebnych do realizacji wewnętrznych audytów bezpieczeństwa.

8.2. W wyniku realizacji prac, opisanych w sekcji **"Testy bezpieczeństwa (etap II)"** Wykonawca dostarczy raport, który zawierać będzie:

- 8.2.1. zakres, metodykę i szczegółowy opis przeprowadzonych prac,
- 8.2.2. opis przyjętego modelu oceny ryzyka,
- 8.2.3. wyniki oceny zgodności z dobrymi praktykami,
- 8.2.4. wyniki identyfikacji luk i wad konfiguracyjnych,
- 8.2.5. analizę wykrytych ryzyk pod kątem bezpieczeństwa informacji,
- 8.2.6. wytyczne i zalecenia co do wdrożenia poprawek.

9. Miejsce realizacji zamówienia

- 9.1. Usługa będzie wykonywana w siedzibie Zamawiającego lub w miejscach przez niego wskazanych lub zdalnie.
- 9.2. Zamawiający będzie wskazywał zapotrzebowanie na testy w 2026 r., z uwzględnieniem wcześniejszego powiadomienia i ustalenia daty wykonania poszczególnych testów wynikających z zapotrzebowania realizacji wymagań wskazanych w pkt 5 i 6.

W miejscach, gdzie w opisie wskazano znaki towarowe, patenty lub pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę, Zamawiający dopuszcza składanie ofert równoważnych. Za rozwiązanie „równoważne” uznany zostanie przedmiot zamówienia, którego zaoferowane parametry będą nie gorsze (niższe) niż parametry rozwiązania opisanego w Ogłoszeniu o zamówieniu (w załączniku nr 1 opis przedmiotu zamówienia), a zastosowanie ich gwarantować będzie osiągnięcie efektów końcowych zgodnie z założeniami i warunkami określonymi w Ogłoszeniu o zamówieniu. W miejscach, gdzie w opisie wskazano normy, Zamawiający dopuszcza rozwiązania równoważne. Wykonawca, który powołuje się na rozwiązania równoważne, jest zobowiązany udowodnić w ofercie, że oferowane przez niego rozwiązanie w równoważnym stopniu spełnia wymagania określone przez Zamawiającego w opisie przedmiotu zamówienia. W takim przypadku Wykonawca załącza do oferty wykaz rozwiązań równoważnych stosownie wraz z jego opisem lub normami oraz dowody potwierdzające równoważność.