

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest świadczenie usługi monitorowania dostępności i działania usług e- Zdrowia wraz z usługą wsparcia technicznego.
2. **Zakres zamówienia:**
 - 2.1. Uruchomienie usługi i przekazanie niezbędnych poświadczeń administratora do CeZ osobie wskazanej w umowie,
 - 2.2. świadczenie usługi monitorowania dostępności i działania usług udostępnianych obywatelom przez Centrum e-Zdrowia (CeZ),
 - 2.3. zapewnienie pełnego wsparcia technicznego oraz dokumentacji użytkownika i administratora,
 - 2.4. integracja rozwiązania z systemami monitorowania (np. Zabbix, Grafana),
 - 2.5. wsparcie dla logowania za pomocą Profilu Zaufanego,
 - 2.6. monitorowanie dostępności stron internetowych oraz usług z różnych lokalizacji (krajowych i zagranicznych),
 - 2.7. zastosowanie wielu metod weryfikacji dostępności (np. Ping, Curl, Fullpage),
 - 2.8. raportowanie dostępności usług oraz generowanie alertów w czasie rzeczywistym,
 - 2.9. monitorowanie integralności usług rządowych udostępnionych obywatelom przez CeZ.
 - 2.10. Możliwość wykorzystania minimum 300 monitorów oraz 30 scenariuszy testowych umożliwiających testowanie niestandardowych (spoza puli dostępnej w ramach usługi) funkcjonalności.

Całość przedmiotu zamówienia będzie dalej zwana „Usługą”.

3. Termin realizacji zamówienia:

- 3.1. Okres świadczenia usługi wynosi 12 lub 24 miesiące, licząc od dnia podpisania umowy lub innego terminu wskazanego w jej treści.
- 3.2. Uruchomienie Usługi: Wykonawca zobowiązany jest do uruchomienia Usługi w terminie do 14 dni od zawarcia umowy, w tym do przekazania niezbędnych poświadczeń administratora do CeZ osobie wskazanej w umowie oraz dostarczenia pełnej dokumentacji technicznej i użytkowej. Poświadczenia muszą być przekazane w sposób bezpieczny i umożliwiać ich późniejszą zmianę lub cofnięcie przez Zamawiającego.

4. Wymagania: Poniżej przedstawiono szczegółowe wymagania, które muszą zostać spełnione przez Wykonawcę w ramach realizacji Usługi**4.1. Wymagania funkcjonalne:**

- 4.1.1. Logowanie i autoryzacja: Narzędzie musi wspierać logowanie za pomocą Profilu Zaufanego. Logowanie powinno umożliwiać jednoznaczną identyfikację użytkownika oraz być zgodne z obowiązującymi przepisami dotyczącymi uwierzytelniania usług publicznych. Wykonawca odpowiada za zapewnienie odpowiednich uprawnień do korzystania z Profilu Zaufanego.

4.1.2. Rola użytkowników: Narzędzie powinno umożliwiać definiowanie i zarządzanie rolami użytkowników, takimi jak administratorzy, operatorzy, audytorzy, z różnym zakresem dostępnych funkcji i poziomów uprawnień. System musi umożliwiać dynamiczne nadawanie, modyfikowanie i cofanie ról oraz rejestrować historię zmian uprawnień w formie logów audytowych dostępnych dla Zamawiającego.

5. Monitorowanie stron i usług:

5.1. Usługa powinna dostarczać minimum poniższe metody monitorowania, z możliwością konfiguracji ich parametrów (np. częstotliwości testów, lokalizacji, nagłówków HTTP) przez Zamawiającego:

5.1.1.Ping: Sprawdzanie dostępności usług za pomocą protokołu ICMP, z możliwością rejestrowania wyników testów oraz generowania alertów w przypadku braku odpowiedzi.

5.1.2.Curl: Weryfikacja dostępności usług za pomocą zapytań HTTP i HTTPS (w tym możliwość przekazania dodatkowych nagłówków HTTP, np. dla autoryzacji).

5.1.3.Fullpage: Monitorowanie pełnych stron internetowych, w tym sprawdzanie, poprawności ładowania stron oraz dostępności wszystkich istotnych zasobów (np. obrazy, skrypty), z możliwością symulacji działania na różnych urządzeniach i przeglądarkach.

5.1.4. Obsługa protokołów: Wszystkie metody monitorowania muszą wspierać zarówno HTTP, jak i HTTPS z odpowiednim szyfrowaniem oraz umożliwiać weryfikację ważności certyfikatów SSL/TLS.

5.1.5. Monitorowanie różnych usług: Narzędzie musi wspierać monitorowanie zarówno usług statycznych, jak i dynamicznych (np. usługi oparte na API, aplikacje webowe) z możliwością autoryzacji do usług po API oraz testowania odpowiedzi na zapytania z parametrami.

6. Wymagania w zakresie wysokiej dostępności:

6.1. Narzędzie musi zapewnić dostępność Usługi na poziomie nie niższym niż 99,5% w skali miesiąca, zgodnie z zasadami SLA, co oznacza, że usługa musi być dostępna przez 99,5% czasu w danym okresie. Wykonawca zobowiązany jest do comiesięcznego raportowania poziomu dostępności.

6.1.1.1. Wzór: $\text{Dopuszczalny czas przestoju} = (100\% - 99,5\%) * \text{całkowity czas w minutach}$

6.1.1.2. Przykład: Dla miesiąca liczącego 30 dni (43 200 minut), dopuszczalny czas przestoju wynosi 216 minut.

6.2. Monitoring dostępności usługi: Narzędzie musi posiadać mechanizmy, które pozwolą na automatycznego testowania dostępności samego systemu monitorującego, z możliwością rejestrowania wyników testów oraz generowania alertów w przypadku wykrycia niedostępności.

7. Wymagania w zakresie integracji:

- 7.1. Narzędzie musi umożliwiać integrację z systemami monitorowania wykorzystywanymi przez Zamawiającego, w szczególności z Zabbix oraz Grafana, poprzez interfejsy API (RESTful lub inne zgodne z dokumentacją techniczną tych systemów), umożliwiające:
- 7.1.1. Odbieranie i przysyłanie danych dotyczących dostępności usług, stron internetowych oraz komponentów systemowych, w formacie JSON lub XML, z możliwością konfiguracji zakresu przesyłanych danych (np. czas odpowiedzi, status HTTP, lokalizacja testu).
 - 7.1.2. tworzenie wykresów, dashboardów z dostępności usług oraz ich szczegółowych parametrów w Grafanie, prezentujących aktualny oraz historyczny stan dostępności usług, z możliwością filtrowania według lokalizacji, typu usługi, czasu oraz poziomu dostępności. Dashboardy muszą być dynamiczne, aktualizowane w czasie rzeczywistym i umożliwiać eksport danych do formatu CSV oraz PDF.
 - 7.1.3. automatyczne przysyłanie danych o dostępności usług do Zabbix w celu centralnego monitorowania infrastruktury IT Zamawiającego
 - 7.1.4. Zgodność z polityką bezpieczeństwa CeZ – integracja musi odbywać się z wykorzystaniem bezpiecznych kanałów komunikacji (np. HTTPS z TLS 1.2 lub wyższym), z uwierzytelnianiem API (np. tokeny, klucze API, OAuth2) oraz rejestrowaniem wszystkich operacji integracyjnych w logach systemowych.

8. Wymagania w zakresie zarządzania użytkownikami:

- 8.1. Narzędzie musi umożliwiać tworzenie imiennych kont czasowych (np. do wykonania audytu, jednorazowego sprawdzenia dostępności) z możliwością określenia czasu ważności konta. Konta te muszą być automatycznie dezaktywowane po upływie zdefiniowanego okresu.
- 8.2. Usługa musi umożliwiać wydzielenie kont dedykowanych Zamawiającemu w tym dla Administratora Zamawiającego, Operatora oraz Audytora, z możliwością nadawania i modyfikowania uprawnień.
- 8.3. Administratorzy Zamawiającego muszą mieć możliwość pełnej kontroli nad kontami użytkowników, w tym zarządzania dostępem, nadawania, modyfikowania i cofania odpowiednich ról i uprawnień, przeglądania historii zmian uprawnień oraz rejestrowania działań podejmowanych przez użytkowników w systemie w formie logów audytowych dostępnych w panelu administracyjnym.

9. Wymagania w zakresie dostępności:

- 9.1. Narzędzie musi działać w popularnych przeglądarkach internetowych (takich jak Chrome, Firefox, Safari, Edge) zarówno na urządzeniach klasy PC i mobilnych (Android, iOS).
- 9.2. Interfejs użytkownika musi być w pełni responsywny, zapewniając płynne działanie na urządzeniach mobilnych, w tym dostosowanie rozmiarów interfejsu oraz układu komponentów do różnych rozdzielczości ekranu, z zachowaniem czytelności i funkcjonalności.

10. Wymagania dotyczące monitoringu dostępności usług:

10.1. Narzędzie musi umożliwiać monitorowanie dostępności usług z minimum dwóch lokalizacji:

10.1.1. Lokalizacja stacjonarna – z terytorium Polski oraz zagranicy m.in. terytorium UE

10.1.2. Lokalizacja mobilna – umożliwiająca symulację dostępu do usług przez urządzenia mobilne, testowanie różnic w dostępności między połączeniami mobilnymi a stacjonarnymi.

10.2. Możliwość wyboru lokalizacji musi być dostępna w panelu administratora, umożliwiając wybór odpowiednich lokalizacji dla poszczególnych testów dostępności.

11. Wymagania dotyczące panelu Operatora:

11.1. Panel Operatora musi być dostępny za pomocą przeglądarki internetowej i umożliwiać:

11.1.1. zarządzanie monitorowanymi usługami,

11.1.2. konfigurację alarmów i powiadomień.

11.1.3. generowaniem raportów dostępności

11.2. Interfejs panelu Operatora musi być intuicyjny, ergonomiczny i zgodny z zasadami UX, z możliwością filtrowania danych i dostosowania widoku do roli użytkownika.

12. Wymagania dotyczące raportowania

12.1. Narzędzie musi umożliwiać generowanie cyklicznych raportów dostępności usług minimum w zakresie:

12.1.1. raporty dostępności na poziomie godzinowym, dziennym, tygodniowym oraz miesięcznym (z możliwością parametryzacji częstotliwości generowania raportów)

12.1.2. raporty muszą zawierać zarówno dane tekstowe, jak i graficzne (wykresy, tabele dostępności)

12.1.3. raporty muszą być dostępne w formacie PDF oraz CSV

12.2. Użytkownicy muszą mieć możliwość dostosowywania szablonu generowanych raportów, wybierając monitorowane usługi oraz przedziału czasu.

13. Wymagania dotyczące audytowania prób logowania – dostępne z poziomu panelu Operatora:

13.1. Wszystkie próby logowania do systemu muszą być udokumentowane w postaci:

13.1.1. filmów (z nagraniem próby logowania)

13.1.2. zrzutów ekranów (dowody weryfikacji procesu logowania),

13.1.3. Plików HAR (do analizy szczegółowych informacji o ruchu HTTP).

13.2. Materiały te muszą być dostępne natychmiastowo po próbie logowania.

- 13.3. Materiały muszą być przechowywane i dostępne z możliwością ich pobrania dla Operatora przez okres m.in. 3 miesięcy od daty wystąpienia.

14. Wymagania dotyczące alertów i powiadomień

- 14.1. Usługa musi wspierać alerty „push” oraz dźwiękowe powiadomienia w przeglądarkach internetowych.
- 14.2. Usługa musi wysyłać powiadomienia m.in. poprzez:
- 14.2.1. Wysyłanie powiadomień drogą SMS na zdefiniowane numery telefonu (minimum 10 numerów) o awariach lub problemach z dostępnością usług.
 - 14.2.2. Wysyłanie powiadomień e-mail o statusie usług, awariach lub niedostępności.
 - 14.2.3. Wysyłanie na MS Teams powiadomień o awariach lub statusie usług wysyłane na kanały komunikacyjne w MS Teams przez webhooki.
 - 14.2.4. Alerty muszą być wysyłane w czasie rzeczywistym.

15. Wymagania dotyczące raportów dostępności:

- 15.1. Usługa musi umożliwiać tworzenie dashboardów, które prezentują aktualny stan monitorowanych usług oraz ich dostępność w formie wykresów, tabel i innych widoków wizualnych.
- 15.2. Dashboardy muszą umożliwiać dynamiczne aktualizowanie danych rzeczywistych oraz filtrowanie według różnych parametrów, takich jak czas, lokalizacja, usługi, eksport danych do PDF/CSV, personalizację widoku przez użytkownika.

16. Wymagania techniczne:

- 16.1. Wykorzystywane narzędzie niezbędne do wykonania Usługi przez Wykonawcę musi zapewniać pełną kontrolę nad dostępem i bezpieczeństwem.
- 16.2. Wykorzystywane narzędzie niezbędne do wykonania Usługi musi zapewniać szyfrowanie danych w transmisji (SSL/TLS), stosowanie zaawansowanych mechanizmów ochrony przed atakami (DDoS, brute force, etc.), a także być zgodne z obowiązującymi przepisami dotyczącymi Ochrony Danych Osobowych i bezpieczeństwa informacji (Ustawa z dnia 10 maja 2018 o Ochronie Danych Osobowych).

17. Wymagania dotyczące wsparcia i dokumentacji

- 17.1. Wykonawca musi zapewnić wsparcie techniczne w trybie 24/7, z czasem reakcji nie dłuższym niż 2 godziny dla zgłoszeń krytycznych, w przypadku problemów z dostępnością lub działaniem narzędzia.
- 17.2. Wykonawca musi dostarczyć pełną Dokumentację Użytkownika, Dokumentację Administratora oraz Dokumentację API (w formacie OpenAPI lub równoważnym), Instrukcje wdrożeniowe i eksploatacyjne.

Osoba sporządzająca: Anna Lerska-Linkiewicz