

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest świadczenie Usługi monitorującej dostępność rządowych udostępnionych obywatelom przez Centrum e-Zdrowia (CeZ) serwisów internetowych, z pełnym wsparciem dla logowania za pomocą profilu zaufanego. Usługa ma umożliwiać monitorowanie dostępności stron internetowych oraz funkcjonalności z różnych lokalizacji, z wieloma metodami weryfikacji, raportowaniem dostępności i generowaniem alertów w czasie rzeczywistym. Narzędzie ma być także zintegrowane z systemami monitorowania, takimi jak Zabbix oraz Grafana. Przedmiot zamówienia zwany będzie dalej „Usługą”.

1. Termin realizacji usługi:

12 miesięcy od dnia uruchomienia usługi

2. Termin uruchomienia Usługi

Do 2 tygodni (14 dni) od podpisania umowy.

3. Zamówienie obejmuje:

- 3.1. Uruchomienie Usługi i przekazanie niezbędnych poświadczeń administratora do CeZ osobie wskazanej w umowie
- 3.2. Przekazanie niezbędnej dokumentacji

Usługa - wymagania.

4. Wymagania funkcjonalne

- 4.1. Możliwość podstawowego monitorowania serwisów internetowych dla minimum 100 adresów.
- 4.2. Możliwość uruchomienia 3 scenariuszy logowania do serwisów z wykorzystaniem różnych metod:
 - 4.2.1. Profil Zaufany;
 - 4.2.2. Bankowość elektroniczna;
 - 4.2.3. Certyfikat kwalifikowany.
- 4.3. Wykonawca odpowiada za zapewnienie niezbędnych uprawnień do korzystania z metod z punktu powyżej.
- 4.4. Role użytkowników portalu: Narzędzie powinno umożliwiać definiowanie różnych ról użytkowników, takich jak administratorzy, operatorzy, z różnym zakresem dostępnych funkcji i poziomów uprawnień.

5. Monitorowanie serwisów internetowych

5.1. Usługa powinna dostarczać minimum poniższe metody monitorowania:

5.1.1.Ping: Sprawdzanie dostępności serwisu za pomocą protokołu ICMP.

5.1.2.Curl: Weryfikacja dostępności serwisu 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, czy strony ładują się poprawnie oraz czy są dostępne wszystkie istotne zasoby (np. obrazy, skrypty).

5.1.4.Obługa protokołów: Wszystkie metody monitorowania muszą wspierać zarówno HTTP, jak i HTTPS z odpowiednim szyfrowaniem.

5.1.5.Monitorowanie różnych serwisów: Narzędzie musi wspierać monitorowanie zarówno stron statycznych, jak i dynamicznych (np. usługi oparte na API, aplikacje webowe).

6. Wymagania w zakresie wysokiej dostępności

6.1. Narzędzie musi zapewnić SLA 99,5% co oznacza, że Usługa musi być dostępna przez 99,5% czasu w danym okresie rozliczeniowym.

Wzór:

Dopuszczalny czas przestoju = $(100\% - 99,5\%) \cdot \text{całkowity czas w minutach}$

7. Wymagania w zakresie integracji

7.1. Narzędzie musi umożliwiać integrację z systemem Zabbix oraz Grafana poprzez standardowe API, pozwalając na:

7.1.1.otrzymywanie i wysyłanie danych o dostępności stron i monitorowanych stronach.

7.1.2.tworzenie wykresów i dashboardów z dostępności serwisów oraz ich szczegółowych parametrów w Grafanie.

7.1.3.automatyczne przysyłanie danych o dostępności usług do Zabbix w celu centralnego monitorowania infrastruktury.

8. Wymagania w zakresie zarządzania użytkownikami

8.1. Narzędzie musi umożliwiać tworzenie imiennych kont czasowych (np. do wykonania audytu, jednorazowego sprawdzenia dostępności). Konta te mają być automatycznie dezaktywowane po określonym czasie.

8.2. Usługa musi umożliwiać wydzielenie kont dedykowanych Zamawiającemu do administracji udostępnioną Usługą, w tym Administratora Zamawiającego, Operatora – 30 kont imiennych.

8.3. Administratorzy Zamawiającego muszą mieć możliwość pełnej kontroli nad kontami użytkowników, w tym zarządzania dostępem, nadawania odpowiednich ról i uprawnień oraz rejestrowania działań podejmowanych przez użytkowników w systemie.

8.4. Wymagania w zakresie dostępności

8.4.1. Usługa musi działać w popularnych przeglądarkach internetowych zarówno na urządzeniach klasy PC i mobilnych (np. Chrome, Firefox, Safari).

8.4.2. Interfejs użytkownika powinien być w pełni responsywny, zapewniając płynne działanie na urządzeniach mobilnych, w tym dostosowanie rozmiarów interfejsu oraz układu komponentów do różnych rozdzielczości ekranu.

9. Wymagania dotyczące monitoringu dostępności stron

9.1. Narzędzie musi umożliwiać monitorowanie dostępności serwisów z minimum dwóch lokalizacji:

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

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

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

10. Wymagania dotyczące panelu Operatora

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

10.1.1. monitorowanymi stronami,

10.1.2. ustawieniami alarmów i powiadomień,

10.1.3. generowaniem raportów dostępności.

10.2. Interfejs panelu Operatora powinien być intuicyjny i umożliwiać łatwe zarządzanie dostępnymi dla danej roli funkcjami narzędzia.

11. Wymagania dotyczące raportowania

11.1. Usługa musi umożliwiać generowanie cyklicznych raportów dostępności stron minimum w zakresie:

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

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

11.1.3. raporty muszą być dostępne co najmniej w formacie PDF oraz CSV.

11.2. Użytkownicy muszą mieć możliwość dostosowywania szablonu generowanych raportów, wybierając monitorowane strony oraz okres czasu.

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

- 12.1. Wszystkie próby logowania do systemu muszą być udokumentowane w postaci:
 - 12.1.1. filmów (z nagraniem próby logowania),
 - 12.1.2. zrzutów ekranów (dowody weryfikacji procesu logowania),
 - 12.1.3. Plików HAR (do analizy szczegółowych informacji o ruchu HTTP).
- 12.2. Materiały te muszą być dostępne natychmiastowo po próbie logowania.
- 12.3. Materiały powinny być przechowywane i dostępne z możliwością ich pobrania dla Operatora przez okres m.in. 3 miesięcy od daty wystąpienia.

13. Wymagania dotyczące alertów i powiadomień

- 13.1. Usługa musi wspierać alerty „push” oraz dźwiękowe powiadomienia w przeglądarkach internetowych.
- 13.2. Usługa musi wysyłać powiadomienia m.in. poprzez:
 - 13.2.1. Wysyłanie powiadomień drogą SMS na zdefiniowane numery telefonu (minimum 10 numerów) o awariach lub problemach z dostępnością usług;
 - 13.2.2. Wysyłanie powiadomień e-mail o statusie stron w przypadku awarii lub niedostępności;
 - 13.2.3. Wysyłanie na MS Teams powiadomień o awariach lub statusie usług wysyłane na kanały komunikacyjne w MS Teams przez webhooki.

14. Wymagania dotyczące raportów dostępności

- 14.1. Usługa musi umożliwiać tworzenie dashboardów, które prezentują aktualny stan monitorowanych serwisów oraz ich dostępność w formie wykresów, tabel i innych widoków wizualnych.
- 14.2. Dashboardsy muszą umożliwiać dynamiczne aktualizowanie danych rzeczywistych oraz filtrowanie według różnych parametrów, takich jak czas, lokalizacja, serwisy internetowe.

15. Wymagania techniczne

- 15.1. Wykorzystywane narzędzie niezbędne do wykonania Usługi przez Wykonawcę musi zapewniać pełną kontrolę nad dostępem i bezpieczeństwem.
- 15.2. 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).

16. Wymagania dotyczące wsparcia i dokumentacji

- 16.1. Wykonawca musi zapewnić wsparcie techniczne w trybie 24/7 w przypadku problemów z dostępnością lub działaniem narzędzia.
- 16.2. Wymagane jest dostarczenie pełnej Dokumentacji Użytkownika, Dokumentacji Administratora oraz dokumentacji API w terminie nie dłuższym niż 2 tygodnie po podpisaniu umowy.