Wstępny Opis Przedmiotu Zamówienia

Zaprojektowanie i zbudowanie Systemu Monitorowania Jakości Internetu (SMJI) oraz wdrożenie e-usługi pn. *Dostęp do bieżącej informacji o jakości usług IAS*

Urząd Komunikacji Elektronicznej

6 czerwca 2022 r.

wersja 1

Spis treści

1. Definicje

Termin	Definicja
ADR	ang. *Alternative Dispute Resolution* - alternatywne (pozasądowe) systemy, tryby lub metody rozwiązywania sporów
CSIRT	ang. *Computer Security Incident Response Team* zespół reagowania na incydenty związane z bezpieczeństwem komputerowym to centrum ostrzegania i reagowania na ataki komputerowe, przeznaczone dla firm lub administracji, którego informacje są ogólnie dostępne dla wszystkich.
CSU	Centralny System Uwierzytelniania
ESOD	Elektroniczny System Obiegu Dokumentów funkcjonujący w Urzędzie.
E-Usługa	E-usługa p.n. *Dostęp do bieżącej informacji o jakości usług IAS*, udostępniona w ramach realizacji projektu *Dostęp do bieżącej informacji o jakości usług IAS w oparciu o System Monitorowania Jakości Internetu (SMJI)* realizowanego w ramach II osi Programu Operacyjnego Polska Cyfrowa „E-administracja i otwarty rząd", cel szczegółowy nr 2 „Wysoka dostępność i jakość e-usług publicznych", na podstawie porozumienia o dofinansowanie nr POPC.02.01.00-00-0136/21-00.
IAS	ang. *Internet Access Services* – usługi dostępu do Internetu.
ISAC	ang. *Information Sharing and Analysis Center* - Centrum Wymiany i Analizy Informacji, forma partnerstwa publiczno-prywatnego (PPP), stosowana w obszarze cyberbezpieczeństwa wokół różnych sektorów gospodarki, której zadaniem jest zrzeszanie instytucji oraz umożliwianie im wymiany doświadczeń o zagrożeniach.
ISP	ang. *Internet Service Provider* – dostawca usług dostępu do sieci Internet.
KRI	Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, t.j. Dz.U. 2017 poz. 2247.
NBD	ang. *Next Business Day* – termin odnoszący się do naprawy sprzętu w następnym dniu roboczym od zgłoszenia
Projekt	Realizowany przez Zamawiającego projekt p.n. *Dostęp do bieżącej informacji o jakości usług IAS w oparciu o System Monitorowania Jakości Internetu (SMJI)* w ramach II osi Programu Operacyjnego Polska Cyfrowa „E-administracja i otwarty rząd", cel szczegółowy nr 2 „Wysoka dostępność i jakość e-usług publicznych", na podstawie porozumienia o dofinansowanie nr POPC.02.01.00-00-0136/21-00
PT	Przedsiębiorca Telekomunikacyjny, na potrzeby niniejszego dokumentu, przyjmuje się definicję zgodnie z Art. 2. Ustawy PT: Jest to przedsiębiorca lub inny podmiot uprawniony do wykonywania działalności gospodarczej na podstawie odrębnych przepisów, który wykonuje działalność gospodarczą polegającą na dostarczaniu sieci telekomunikacyjnych, świadczeniu usług towarzyszących lub świadczeniu

Termin	Definicja
	usług telekomunikacyjnych, przy czym przedsiębiorca telekomunikacyjny, uprawniony do: – świadczenia usług telekomunikacyjnych, zwany jest „dostawcą usług”, – dostarczania publicznych sieci telekomunikacyjnych lub świadczenia usług towarzyszących, zwany jest „operatorem”;
RODO	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
SLA	ang. Service Level Agreement - umowa o gwarantowanym poziomie świadczenia usług
System, SMJI	System Monitorowania Jakości Internetu – oprogramowanie, urządzenia, usługi i baza danych realizujące cele, założenia i wymagania określone w niniejszym Opisie Przedmiotu Zamówienia.
UK	Użytkownik końcowy, zgodnie z Art. 2 pkt 50 Ustawy PT jest to podmiot korzystający z publicznie dostępnej usługi telekomunikacyjnej lub żądający świadczenia takiej usługi dla zaspokojenia własnych potrzeb. UK mogą być osoby fizyczne lub podmioty gospodarcze, które są usługobiorcami usług IAS.
UKE	Urząd Komunikacji Elektronicznej
Ustawa PT	Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, t.j. Dz.U.2021.576 z późn. zm.

2. Cel zamówienia

Celem zamówienia jest zaprojektowanie i zbudowanie Systemu Monitorowania Jakości Internetu oraz wdrożenie e-usługi pn. *Dostęp do bieżącej informacji o jakości usług IAS* na potrzeby realizacji projektu *Dostęp do bieżącej informacji o jakości usług IAS*[1] *w oparciu o System Monitorowania Jakości Internetu (SMJI)* realizowanego w ramach II osi Programu Operacyjnego Polska Cyfrowa „E-administracja i otwarty rząd”, cel szczegółowy nr 2 „Wysoka dostępność i jakość e-usług publicznych”, na podstawie porozumienia o dofinansowanie nr POPC.02.01.00-00-0136/21-00.

Projektowana e-usługa pozwoli na automatyczną weryfikację i przedstawienie konsumentom lub podmiotom gospodarczym, korzystającym z usługi IAS w postaci ujednoliconej prezentacji zmierzonych parametrów testowanych usług w odniesieniu do wartości deklarowanych przez PT. Ponadto, dzięki zastosowaniu odpowiednich pomiarów pozwoli na przedstawienie przystępnej informacji o użyteczności łącza do określonych zastosowań.

Bieżąca ocena jakości usług nabiera istotnego znaczenia przy wzroście liczby usług cyfrowych oddziałujących na obszary gospodarki a dostarczanych za pośrednictwem sieci. Podstawowy parametr, jakim jest maksymalna przepustowość łącza staje się niewystarczający do oceny rzeczywistej dostępnej

[1] ang. *Internet Access Services* – usługi dostępu do Internetu

przepustowości, stabilności łącza czy opóźnień. Wzrastające wykorzystanie usług wideokonferencji, oparte ze względów wydajnościowych na protokołach UDP jest jednym ze szczególnie wrażliwych przypadków, w których brak stabilności łącza internetowego powoduje utratę informacji w czasie rzeczywistym.

Z punktu widzenia Zamawiającego jako regulatora rynku telekomunikacyjnego, istnieje potrzeba wsparcia obsługi procedur reklamacyjnych prowadzonych w klasyczny sposób a obejmujących około 2,5 tysiąca wniosków w skali roku. Dodatkowo, działania regulatora o charakterze informacyjnym obejmują około 15 tysięcy zgłoszeń w skali roku. W obydwu obszarach, Zamawiający oczekuje usprawnienia obsługi procesów przez włączenie ich do e-usługi realizowanej w trybie transakcyjnym.

Monitorowanie jakości usług dostępu do sieci Internet ma dostarczyć dodatkowych informacji dla Przedsiębiorców Telekomunikacyjnych wykorzystywanych w procesie planowania inwestycji i rozwoju infrastruktury telekomunikacyjnej, niezależnie od medium transmisyjnego.

2.1. Krótkie streszczenie Projektu

Przedmiotem projektu jest E-Usługa pod nazwą *Dostęp do bieżącej informacji o jakości usług dostępu do Internetu (IAS – ang. Internet Access Service)*. Projektowana E-Usługa pozwoli w szczególności na automatyczną weryfikację i przedstawienie Użytkownikom Końcowym, korzystającym z usługi IAS zmierzonych parametrów testowanych usług a także odniesienie ich do wartości deklarowanych przez Przedsiębiorców Telekomunikacyjnych. Jednocześnie, usługa dostarczy Użytkownikom Końcowym:

1. Dedykowane urządzenia pomiarowe - próbniki konsumenckie badające parametry ilościowe (takie jak prędkość łącza, opóźnienie oraz zmienność opóźnienia) oraz parametry jakościowe (takie jak klasy QoS, bezpieczeństwo łącza oraz analiza ruchu i ataków na łącze). Będą one bezpłatnie użyczane przez UKE.
2. Próbniki sieciowe, instalowane w węzłach sieci, badające parametry działania sieci i stanowiące element komplementarny w stosunku do próbników konsumenckich. Próbniki będą certyfikowane przez niezależny podmiot certyfikujący.

SMJI będzie zarządzany i obsługiwany przez UKE.

E-Usługa zapewni powszechny dostęp do bieżącej informacji o jakości oraz bezpieczeństwie usług IAS dla Użytkowników Końcowych dzięki zastosowaniu sieci próbników oraz narzędzi pozwalających na analizę zbieranych danych. E-Usługa będzie obejmowała dostęp dla:

- Przedsiębiorców Telekomunikacyjnych (typ A2B),
- Użytkowników Końcowych (typ A2C).

E-Usługa będzie obejmowała udostępnienie próbników konsumenckich i sieciowych, serwis internetowy wraz z aplikacjami pomiarów, eksploracji danych, analizy statystycznej, raportowania i wizualizacji wyników na indywidualnym, uwierzytelnionym koncie dedykowanym dla danego użytkownika, poprzez graficzny interfejs użytkownika umożliwiający wykorzystywanie funkcji interaktywnej mapy.

E-usługa będzie dostarczała urządzenia oraz oprogramowanie pozwalające na:

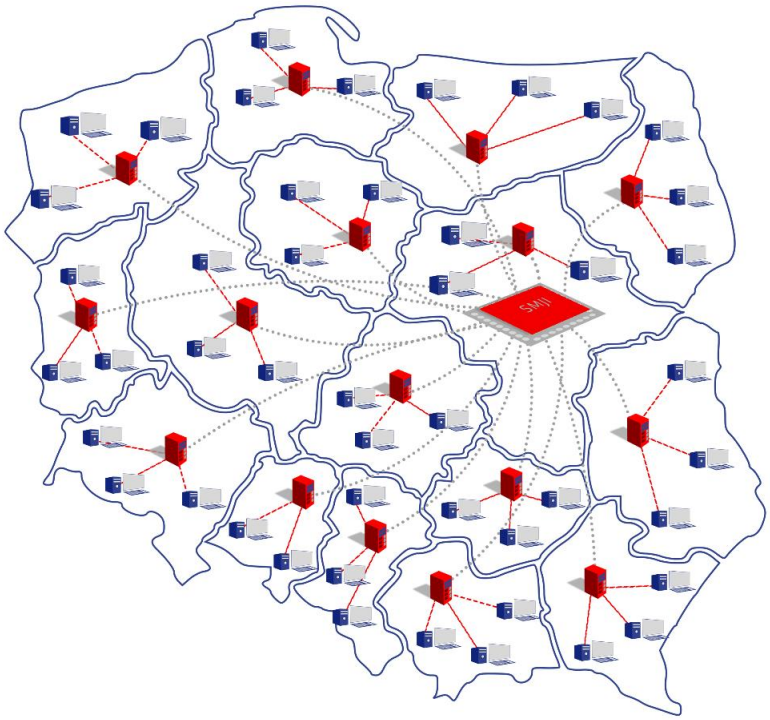
1. przeprowadzanie certyfikowanych pomiarów łącza za pomocą sieci próbników;
2. badanie ilościowe łącza (w tym w postaci ciągłej):
    a. prędkość łącza,
    b. latencja na łączu,
    c. liczba utraconych pakietów,

d. wyznaczanie wartości jednoznacznych, ustandaryzowanych metryk, np. określonych przez rekomendację ITU-T Y.1540[2], takich jak:
    i. opóźnienie przekazu pakietów – IPTD (IP Packet Transfer Delay),
    ii. zmienność opóźnienia przekazu pakietów – IPDV (IP Packet Delay Variation),
    iii. poziom strat pakietów – IPLR (IP Packet Loss Ratio),
    iv. poziom błędnych pakietów – IPER (IP Packet Error Ratio),
    v. przepływność na poziomie pakietów – IPPT (IP Packet Throughput),
    vi. przepływność bajtowa IPOT (Octet-based IP Packet Throughput),
    vii. dostępność usługi IP (IP service availability),
e. wyznaczanie wartości jednoznacznych, ustandaryzowanych metryk, np. określonych przez IETF IPPM (IP Performance Metrics) Working Group[3], takich jak:
    i. dostępność (connectivity),
    ii. opóźnienie OWD (One Way Delay),
    iii. zmienność opóźnienia przekazu pakietów IPDV (IP Packet Delay Variation),
    iv. opóźnienie pakietów w pętli (Round Trip Delay),
    v. straty pakietów OWL (One Way Packet Loss),
f. dodatkowe pomiary ilościowe zidentyfikowane na etapie analizy.

3. badanie jakościowe łącza i usługi:
    a. badanie i klasyfikacja jakości usługi w oparciu o rekomendację ITU-T Y.1541[4],
    b. bezpieczeństwo łącza,
    c. analiza ataków na łącze,
        i. ataki DDoS,
        ii. ataki DoS,
        iii. ataki na protokoły trasowania (BGP, vlan spoofing oraz inne),
        iv. pozostałe ataki na łącze.
4. badanie statystyczne łącza (uwzględniające badania ilościowe oraz jakościowe), mogące posłużyć jako wejście do procesu reklamacji Użytkownika Końcowego oraz raportowania PT.

Aplikacje E-Usługi realizowane będą za pomocą Systemu Monitorowania Jakości Internetu (SMJI) poprzez stacjonarne i mobilne urządzenia IT oraz specjalistyczne próbniki pomiarowe, zainstalowane u Użytkowników Końcowych (próbniki konsumenckie) oraz węzłach PT (próbniki sieciowe), w sieci Internet na terenie kraju. Dane i wyniki prowadzonych pomiarów będą gromadzone w centralnej bazie danych obsługiwanej w systemie 24h/7d. SMJI będzie przygotowany na pracę w reżimie big data. W odróżnieniu od obecnych rozwiązań, będzie on oferował szczegółowe wyniki online klientom indywidualnym oraz instytucjonalnym.

[2] Recommendation ITU-T Y.1540, Internet protocol data communication service – IP packet transfer and availability performance parameters (12/2019), [https://www.itu.int/rec/T-REC-Y.1540]
[3] Dokumenty RFC opracowywane w ramach grupy IETF IPPM dostępne w ramach repozytorium https://datatracker.ietf.org/wg/ippm/documents/
[4] Recommendation ITU-T Y.1541, Network performance objectives for IP-based services (12/2011), [https://www.itu.int/rec/T-REC-Y.1541]



Rysunek 1 - Koncepcja monitorowania jakości usług IAS z użyciem rozproszonej sieci próbników

W ramach funkcjonalności SMJI możliwa będzie dokładna analiza parametrów jakościowych oraz ilościowych oferowanych przez PT w celu podjęcia świadomego wyboru operatora usług IAS. Dodatkowo, pomiary realizowane przez certyfikowane próbniki będą mogły stanowić niepodważalną podstawę w procesie reklamacyjnym klienta w stosunku do nieprzestrzegania parametrów jakościowych oraz ilościowych przez PT.

2.1.1. Interesariusze Projektu i E-Usługi

Interesariuszami Projektu a w szczególności jego głównego produktu w postaci E-Usługi są:

1. Użytkownicy Końcowi (konsumenci lub podmioty gospodarcze, korzystające z usługi IAS).
2. Przedsiębiorcy Telekomunikacyjni dostarczający usługi IAS.
3. Prezes Urzędu Komunikacji Elektronicznej – Urząd Komunikacji Elektronicznej.

2.2. Cele strategiczne Projektu

Budowa Systemu Monitorowania Jakości Internetu i wdrożenie opartej na nim E-Usługi stanowi główny element realizacji Projektu, wpisującego się w następujące dokumenty strategiczne:

1. Program Zintegrowanej Informatyzacji Państwa[5], cel: Zwiększenie jakości oraz zakresu komunikacji między obywatelami i innymi interesariuszami a państwem (pkt. 4.2.1 Programu).
2. Program Operacyjny Polska Cyfrowa[6], cel szczegółowy nr 2: Wysoka dostępność i jakość e-usług publicznych w ramach Osi priorytetowej II. *E-administracja i otwarty rząd*.

[5] Program Zintegrowanej Informatyzacji Państwa, Cyfryzacja KPRM, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/cyfryzacja/program-zintegrowanej-informatyzacji-panstwa

[6] Program Polska Cyfrowa 2014-2020, https://www.polskacyfrowa.gov.pl/strony/o-programie/dokumenty/program-polska-cyfrowa-2014-2020/

3. Strategia na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.)[7], obszar: E-państwo, kierunek Interwencji: Budowa i rozwój e-administracji – orientacja administracji państwa na usługi cyfrowe.
4. *Strategia Sprawne i Nowoczesne Państwo 2030*[8] (projekt)[9], cel szczegółowy III. *Podniesienie sprawności realizacji zadań państwa poprzez wykorzystanie technologii cyfrowych i zmianę sposobu działania stosownie do możliwości, jakie stwarza technologia* (str. 51 projektu strategii).

2.3. Cele szczegółowe zamówienia

Realizacja niniejszego zamówienia a w szczególności Budowa Systemu Monitorowania Jakości Internetu i wdrożenie opartej na nim E-Usługi ma na celu:

CS-1. Dostarczenie E-Usługi dla konsumenta oraz operatorów, pozwalających na próbkowanie oraz mierzenie w czasie rzeczywistym sieci operatorskich a także sieci klienckich konsumentów końcowych.

CS-2. Dostarczenie E-Usługi dla konsumenta pozwalającej na ocenę jakości usług IAS w czasie rzeczywistym.

CS-3. Podwyższenie bezpieczeństwa oraz konkurencyjności PT na skutek zbierania oraz dostarczania informacji z zakresu bezpieczeństwa.

CS-4. Umożliwienie wykrywania oraz raportowania zdarzeń z zakresu bezpieczeństwa oraz ataków na sieci operatorskie oraz na sieci klienckie.

CS-5. Umożliwienie przekazywania danych bezpieczeństwa do CSIRT poziomu krajowego.

CS-6. Zapewnienie możliwości zdalnej realizacji spraw z zakresu jakości usług IAS jako rozwiązanie adekwatne do sytuacji nadzwyczajnych, jaką jest np. pandemia COVID-19.

CS-7. Zapewnienie dostępu do niezaprzeczalnych informacji o faktycznej jakości świadczonych usług IAS o odpowiedniej mocy dowodowej w przypadku postępowania reklamacyjnego, przed Prezesem UKE lub sądem.

CS-8. Zapewnienie możliwości zareklamowania niezgodności parametrów dostarczanej usługi z deklarowanymi w trybie ADR, oraz udzielenia odpowiedzi zwrotnej przez PT do konsumenta.

CS-9. Zapewnienie dostępu do informacji o bezpieczeństwie sieci operatorów oraz konsumentów końcowych, w tym możliwości raportowania w czasie rzeczywistym o zagrożeniach oraz atakach skierowanych w operatorów PT oraz klientów końcowych.

2.4. Szczegółowe potrzeby i problemy, które adresuje E-Usługa

Wdrażana E-Usługa a co za tym idzie narzędzie informatyczne w postaci Systemu odpowiadają potrzebom oraz powinny realnie przyczynić się do rozwiązania wymienionych niżej, zidentyfikowanych

[7] Informacje o Strategii na rzecz Odpowiedzialnego Rozwoju, Ministerstwo Funduszy i Polityki Regionalnej, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/fundusze-regiony/informacje-o-strategii-na-rzecz-odpowiedzialnego-rozwoju

[8] Strategia Sprawne i Nowoczesne Państwo 2030 (SSiNP 2030), Portal Interoperacyjności i Architektury, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/ia/strategia-sprawne-i-nowoczesne-panstwo-2030-ssnip2

[9] Projekt uchwały Rady Ministrów w sprawie przyjęcia strategii „Sprawne i Nowoczesne Państwo 2030", nr w wykazie prac ID63, Ministerstwo Spraw Wewnętrznych i Administracji, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/mswia/projekt-uchwaly-rady-ministrow-w-sprawie-przyjecia-strategii-sprawne-i-nowoczesne-panstwo-2030

przez Zamawiającego w procesie przygotowania Projektu problemów a co najmniej wpłynąć na poprawę sytuacji interesariuszy:

Tabela 1 - Szczegółowe potrzeby, które adresuje E-Usługa

Interesariusz	**Zidentyfikowana potrzeba**
UK Użytkownicy Końcowi (konsumenci lub podmioty gospodarcze, korzystające z usługi IAS)	1) Potrzeba dostępu do wysokiej jakości usług IAS, której faktyczne parametry jakości są zgodne z deklarowanymi wartościami tych parametrów. 2) Potrzeba dostępu do informacji o faktycznej jakości świadczonych usług IAS o odpowiedniej mocy dowodowej w przypadku postępowania reklamacyjnego lub przed Prezesem UKE. 3) Potrzeba dostępu do informacji na temat jakości publicznie dostępnych usług IAS poszczególnych PT. 4) Konieczność zapewnienia bezpieczeństwa konsumentom poprzez monitorowanie usług pod kątem możliwego, niekorzystnego oddziaływania na bezpieczeństwo obywatela, gospodarkę za pośrednictwem cyfrowych usług oferowanych przez przedsiębiorców za pośrednictwem PT. 5) Uproszczenie realizacji pomiaru certyfikowanego poprzez zastosowanie próbnika konsumenckiego, wykonującego pomiar w sposób zautomatyzowany.

Tabela 2 - Szczegółowe problemy, które adresuje E-Usługa

Interesariusz	**Zidentyfikowany problem**
UK Użytkownicy Końcowi (konsumenci lub podmioty gospodarcze, korzystające z usługi IAS)	Dane wykorzystywane przez Prezesa Urzędu Komunikacji Elektronicznej jako organu regulacyjnego w zakresie działalności telekomunikacyjnej podczas postępowań odwoławczych okazują się wystarczającym dowodem do podtrzymania decyzji Prezesa UKE. W postępowaniach sądowych brakuje wiarygodnych, niezaprzeczalnych i możliwych do zweryfikowania danych.
PT Przedsiębiorcy Telekomunikacyjni dostarczający usługi IAS	Brak narzędzi do automatycznej publikacji danych ze sprawozdań składanych przez przedsiębiorców telekomunikacyjnych oraz prezentacji w ujednoliconej formie, pozwalającej na ocenę deklarowanego poziomu jakości usług IAS w sytuacji połączenia sieci oraz rozwiązywania kwestii spornych dotyczących wzajemnego korzystania z sieci telekomunikacyjnej w tym niewykonania lub nienależytego wykonania świadczonych wzajemnie usług telekomunikacyjnych (Art. 32 Ustawy PT).
Prezes Urzędu Komunikacji Elektronicznej – Urząd Komunikacji Elektronicznej	Brak mechanizmów gromadzenia danych o jakości usług IAS na potrzeby ADR oraz ustalenia stałych lub regularnie powtarzających się, istotnych rozbieżności pomiędzy faktycznym poziomem wartości wskaźników jakości usług IAS a wartościami deklarowanymi przez PT w komunikatach publicznych.

2.5. Oczekiwane korzyści i efekty realizacji zamówienia

Zamawiający oczekuje, iż realizacja zamówienia spowoduje:

OKE-1. Dostarczenie E-Usługi dla konsumenta pozwalającej na ocenę jakości oraz bezpieczeństwa usług IAS w czasie rzeczywistym.

OKE-2. Dostęp do danych oraz narzędzi pozwalających na monitorowanie oraz odpytywanie zbiorów danych pod kątem poziomu parametrów ilościowych (np. pasmo łącza) oraz pod kątem parametrów jakościowych (np. bezpieczeństwo łącza) poszczególnych PT.

OKE-3. Zwiększenie dojrzałości konkurencyjnej rynku IAS a co za tym idzie podniesienie poziomu jakości usług IAS dzięki dostępności rzetelnych danych pomiarowych dotyczących parametrów łączy.

OKE-4. Zwiększenie konkurencyjności, a tym samym poziomu ofert dostawców usługi dostępu do Internetu na skutek łatwiejszej możliwości porównywania ich jakości, a także uzyskania wiarygodnych wyników takiego porównania.

OKE-5. Wzrost dostępności, poprawę jakości i niezawodności e-usług publicznych oraz możliwość świadczenia ich w bardziej zaawansowanych formach.

OKE-6. Poszerzenie i ułatwienie dostępu do informacji i korzystania z niej przez UK, PT oraz UKE.

OKE-7. Kontynuację działań Prezesa UKE na rzecz ochrony praw konsumenckich.

OKE-8. Ułatwienie konsumentom dochodzenia roszczeń w obszarze niezgodności usługi IAS w stosunku do parametrów deklarowanych w umowach.

OKE-9. Zapewnienie społeczeństwu możliwości wyszukiwania najkorzystniejszych ofert usługi IAS oraz najbardziej wiarygodnych jej dostawców.

OKE-10. Przyspieszenie realizacji czynności w ramach prowadzonych postępowań zarówno dla klienta jaki i dla UKE.

OKE-11. Redukcję kosztów wynikających m.in. z eliminacji osobistej wizyty w urzędzie czy załatwiania wniosku lub sprawy w formie papierowej.

OKE-12. Wzrost dostępności i transparentności oraz poprawa jakości i niezawodności e-usług publicznych.

OKE-13. Wzrost transparentności i przyjazności administracji a co za tym idzie – wzrost zaufania obywateli do organów państwa.

OKE-14. Wzrost przyjazności administracji i Państwa dla obywateli i przedsiębiorców.

OKE-15. Wygodna i efektywna czasowo realizacja codziennych czynności w obszarze załatwiania spraw urzędowych poprzez możliwość elektronicznej obsługi wniosków składanych do UKE.

OKE-16. Brak konieczności osobistej wizyty w urzędzie oraz brak konieczności sporządzania wniosków w formie papierowej.

OKE-17. Możliwość zdalnej realizacji i kontynuacji wniosków i spraw z zakresu jakości usług IAS jako rozwiązanie adekwatne do sytuacji nadzwyczajnych (np. pandemia COVID-19).

OKE-18. Możliwość oceny wpływu innowacyjnych usług cyfrowych na jakość innych usług dostarczanych do konsumenta.

OKE-19. Lepszy dostęp do wysokiej jakości usługi IAS, której faktyczne parametry jakości są zgodne z deklarowanymi wartościami tych parametrów dla szerokiego grona odbiorców (konsumentów) w trybie transakcyjnym.

OKE-20. Dostęp do niezaprzeczalnych informacji o faktycznej jakości świadczonych usług IAS o odpowiedniej mocy dowodowej w przypadku postępowania reklamacyjnego przed Prezesem UKE lub sądem.

OKE-21. Zmniejszenie liczby osób zaangażowanych w udostępnienie danych na temat jakości publicznie dostępnych usług IAS poszczególnych dostawców i operatorów w testowanej lokalizacji i prezentację w trybie transakcyjnym.

OKE-22. Możliwość poinformowania o niezgodności i zareklamowania niezgodności parametrów dostarczanej usługi z deklarowanymi na podstawie agregowanych danych w trybie ADR oraz udzielenia odpowiedzi zwrotnej przez PT do UK z uwzględnieniem tych danych.

OKE-23. Możliwość zgłoszenia do UKE niezgodności parametrów dostarczanej usługi z deklarowanymi przez PT oraz udostępnienie konsumentowi informacji o wyniku analizy zgłoszenia przy jak najmniejszym zaangażowaniu osób obsługujących ten proces.

OKE-24. Prezentacja użytkownikom E-Usługi zagregowanej, bieżącej liczby zgłoszeń we wskazanej lokalizacji (miejscowość, powiat, województwo) w trybie transakcyjnym.

OKE-25. Kontynuacja działań Prezesa UKE na rzecz bezpieczeństwa konsumentów.

OKE-26. Zapewnienie bezpieczeństwa konsumentom poprzez monitorowanie usług pod kątem możliwego, niekorzystnego oddziaływania na bezpieczeństwo obywatela, gospodarkę za pośrednictwem cyfrowych usług oferowanych przez PT.

OKE-27. Efektywne zwiększenie bezpieczeństwa konsumentów oraz operatorów PT poprzez wprowadzenie narzędzi do monitorowania oraz prewencji zagrożeń bezpieczeństwa sieciowego.

OKE-28. Umożliwienie raportowania oraz wymiany danych z zakresu bezpieczeństwa usług sieciowych, w tym procesu wymiany danych z CSIRT poziomu krajowego.

OKE-29. Dostarczenie rozwiązań pozwalających na monitorowanie, wykrywanie oraz raportowanie zagrożeń bezpieczeństwa w sieciach UK oraz PT.

2.6. Opis stanu obecnego

Prezes UKE, działając w myśl art. 4 ust. 4 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2015/2120 z dnia 25 listopada 2015 r.[10] podjął decyzję o stworzeniu i udostępnieniu użytkownikom końcowym narzędzia do pomiarów jakości IAS (certyfikowany mechanizm monitorowania jakości IAS). Efektem podjętych działań było publiczne udostępnienie 1 grudnia 2018 r. certyfikowanego narzędzia pomiaru jakości usług.

Konieczność wdrożenia mechanizmu monitorowania wynika z przepisów art. 4 ust. 4 Rozporządzenia zgodnie z którym wszelkie stałe lub regularnie powtarzające się istotne rozbieżności pomiędzy faktycznym wykonaniem usługi dostępu do Internetu pod względem prędkości lub innych parametrów jakości usługi, a wykonaniem opisanym przez dostawcę usług dostępu do Internetu - w przypadku gdy odnośne fakty zostały ustalone przy pomocy mechanizmu monitorowania certyfikowanego przez krajowy organ regulacyjny - uznawane są za nienależyte wykonanie do celów uruchomienia środków ochrony prawnej przysługujących konsumentowi zgodnie z prawem krajowym

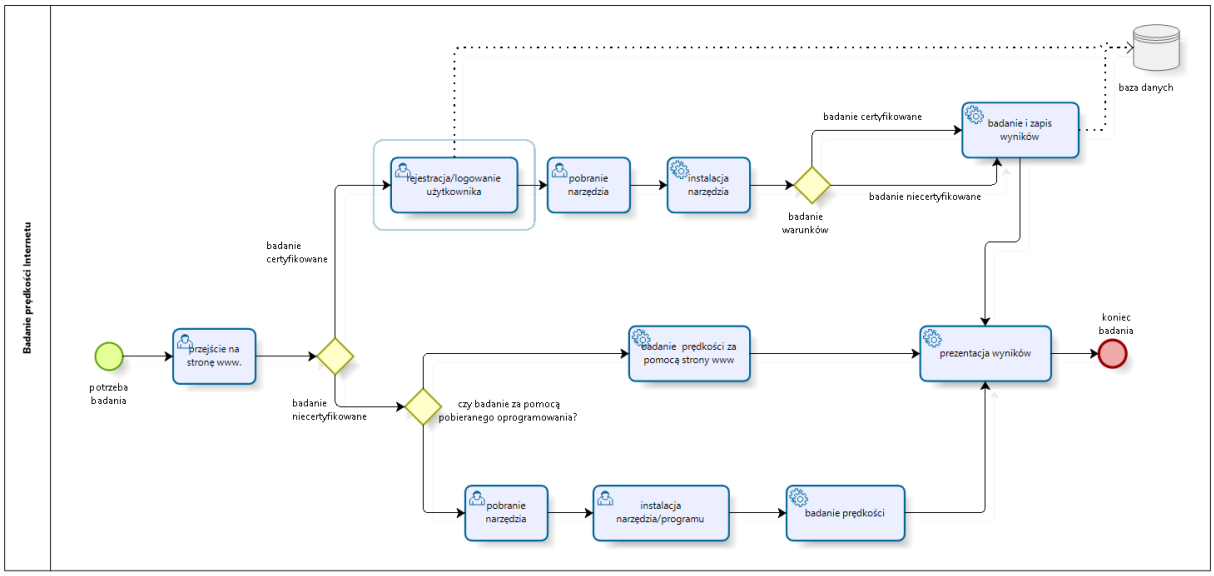
[10] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/2120 z dnia 25 listopada 2015 r. ustanawiające środki dotyczące dostępu do otwartego internetu oraz zmieniające dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, a także rozporządzenie (UE) nr 531/2012 w sprawie roamingu w publicznych sieciach łączności ruchomej wewnątrz Unii, Dz.U. L 310 z 26.11.2015, https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A32015R2120

Mechanizm pomiarowy jest dostępny bezpłatnie pod adresem https://www.pro.speedtest.pl. Składa się z aplikacji na komputery oraz dodatkowych (niecertyfikowanych przez Prezesa UKE) serwisów takich jak aplikacja WEB czy aplikacje mobilne, działające na systemach Android oraz iOS i umożliwiających pomiary w sieciach wykorzystujących technologie radiowe. Dzięki udostępnionej przez Prezesa UKE certyfikowanej aplikacji pomiarowej użytkownicy usług dostępu do Internety mogą sprawdzić prędkości wysyłania i pobierania danych, opóźnienie oraz zmienność opóźnienia w przypadku swojej usługi stacjonarnego Internetu. Mechanizm pomiarowy umożliwia użytkownikom IAS świadczonej w sieci stacjonarnej wykazanie stałych i regularnie powtarzających się rozbieżności pomiędzy faktyczną jakością usługi, a jakością wskazaną przez dostawcę usługi w umowie. Zgodnie z art. 4 Rozporządzenia, pomiar wykonany w sieciach stacjonarnych za pomocą mechanizmu pozwala stwierdzić nienależyte wykonanie umowy i skuteczne dochodzenie roszczeń konsumenta wobec dostawcy usług. W odróżnieniu od innych dostępnych na rynku narzędzi udostępniona aplikacja posiada przymiot certyfikacji przez Prezesa UKE co pozwala na wiarygodny i bezsporny pomiar jakości usługi, wraz z weryfikacją w jakich warunkach pomiary były realizowane. Stwierdzone w wyniku pomiaru rozbieżności parametrów (prędkość transmisji danych, opóźnienia) zawarte w umowie świadczonej usługi z tymi faktycznymi mogą być podstawą w postępowaniu reklamacyjnym klienta wobec dostawcy usług.

Tym samym należy wskazać, iż obecnie dzięki udostępnionej przez Prezesa UKE certyfikowanej aplikacji pomiarowej użytkownicy usług dostępu do Internety mogą sprawdzić prędkości wysyłania i pobierania danych, opóźnienie oraz zmienność opóźnienia w przypadku swojej usługi stacjonarnego internetu.

Mając na uwadze zasadność funkcjonowania certyfikowanego mechanizmu pomiarowego Prezes Urzędu Komunikacji Elektronicznej ponownie certyfikował system pomiarowy PRO Speed Test 1 grudnia 2020 roku na okres kolejnych 2 lat. Do czasu pełnego wdrożenia funkcjonalności pomiarowej Przedmiotu Zamówienia wskazany wyżej Certyfikowany Mechanizm pomiarowy będzie dostępny dla użytkowników. Zakłada się, że co najmniej okresie wdrażania Przedmiotu Zamówienia tj. E-Usługi Certyfikowany Mechanizm będzie dostępny w sposób komplementarny gwarantując w ten sposób nieprzerwany dostęp dla abonentów do wiarygodnego narzędzia pomiarowego jakości usług.

Komplementarność rozwiązania PRO Speed Test w stosunku do SMJI wynika przede wszystkim z pojemności obydwu rozwiązań. W przypadku pierwszego, nie występuje ograniczenie liczby urządzeń, za pomocą których użytkownik może dokonać pomiaru. W przypadku drugiego rozwiązania, liczba jednocześnie wykonywanych pomiarów oraz czas ich rozpoczęcia są zależne od dostępności urządzenia pomiarowego (próbnika konsumenckiego). Czynnikiem przemawiającym za użyciem przez Użytkownika Końcowego próbnika konsumenckiego jest uproszczenie procedury pomiarowej. W przypadku rozwiązania PRO Speed Test, w celu spełnienia warunków pomiaru certyfikowanego, wymagane jest podjęcie i przeprowadzenie przez użytkownika szeregu sprecyzowanych w metodzie działań, weryfikowanych w węźle „badanie warunków" na diagramie procesu pomiaru, Rysunek 2. W ocenie Zamawiającego jest to jeden z powodów, dla którego liczba pomiarów certyfikowanych jest niższa, niż niecertyfikowanych.



Rysunek 2 - Diagram procesu pomiaru dla rozwiązania PRO SpeedTest

2.7. Opis stanu docelowego

E-Usługa obejmuje uruchomienie sieci próbników (sieciowych i konsumenckich) w tym udostępnienie dedykowanych urządzeń pomiarowych - próbników oraz serwis internetowy wraz z aplikacjami pomiarów, eksploracji danych, analizy statystycznej, raportowania i wizualizacji wyników na indywidualnie uwierzytelnionym koncie – dedykowanym dla danego użytkownika (tj. UK i PT) – poprzez graficzny interfejs użytkownika umożliwiający wykorzystywanie funkcji interaktywnej mapy.

Użytkownik Końcowy, który zechce zweryfikować jakość zakupionej przez niego usługi IAS, będzie mógł wybrać interesującą go lokalizację, w której świadczona jest usługa i pobrać dane z bazy SMJI. W przypadku, gdy w tej lokalizacji lub sieci nie będzie certyfikowanego urządzenia pomiarowego (próbnika), będzie mógł zamówić próbnik konsumencki, który zostanie mu udostępniony do instalacji w jego sieci. Dzięki temu będzie mógł uzyskać certyfikowany wynik pomiaru, jednocześnie udostępniając go innym konsumentom korzystającym z usług tego samego dostawcy. Informacja o jakości pomiaru dostępna dzięki bazie SMJI, zostanie zanonimizowana.

Biorąc pod uwagę, że obecnie wykonywane testy konsumenckie (na podstawie Sprawozdania z działalności Prezesa UKE za 2020 r.[11]), które wykonywane aplikacją dostępną z poziomu przeglądarki internetowej pod adresem www.speedtest.pl (np. w samym kwietniu 2020 r. to około 3,8 mln) i aplikacją Internet SpeedTest dostępną na urządzenia mobilne (w kwietniu 2020 r. o koło 822 tys.) były przeprowadzane samodzielnie przez Użytkowników Końcowych i są obarczone: wpływem ich urządzeń końcowych, ograniczeniami planów taryfowych, wykorzystywaniem w sieciach domowych technologii Wi-Fi, liczbą równocześnie aktywnych urządzeń, warunkami propagacji fal radiowych, pozwalają poznać odczuwalną jakość usługi z jakiej korzystają użytkownicy a w mniejszym stopniu wskazują na techniczne możliwości dostarczania usług przez ISP stanowić mogą źródło nieporozumień i być podstawą sporów w których wykorzystywany materiał dowodowy jest podważany przez PT. SMJI pozwoli uwzględnić ww. uwarunkowania, które mogą wpłynąć na uzyskany wynik pomiaru poprzez zastosowanie urządzeń dedykowanych do przeprowadzania pomiarów w postaci próbników.

[11] Sprawozdanie Prezesa UKE za 2020 r., Biuletyn Informacji Publicznej Urzędu Komunikacji Elektronicznej, https://bip.uke.gov.pl/sprawozdania/sprawozdanie-prezesa-uke-za-2020-r-,19.html

Dlatego też, niezależny pomiar za pomocą Systemu Monitorowania Jakości Internetu (SMJI) poprzez typowe, używane na rynku urządzenia IT (stacjonarne i mobilne) oraz certyfikowane konsumenckie próbniki pomiarowe zainstalowane w sieci Internet na terenie kraju i próbniki sieciowe pozwoli na uzyskanie obiektywnego i wiarygodnego wyniku pomiaru parametrów łącza i weryfikację stanu usług świadczonych na tym łączu.

W ramach SMJI, urządzenia oraz algorytmy odpowiedzialne za pomiary bezpieczeństwa będą odpowiadały za wykrywanie oraz zgłaszanie powyższych problemów bezpieczeństwa, umożliwiając reagowanie na zagrożenia w zarodku oraz przekładając się na zwiększenie bezpieczeństwa końcowych sieci użytkowników oraz sieci PT.

SMJI opiera się na pokryciu kraju próbnikami pomiarowymi, które w czasie rzeczywistym mierzą parametry jakości oraz bezpieczeństwa usług IAS oraz końcowych segmentów sieci obsługujących UK. Pomiary będą odbywać się w trybie 24/7, a wyniki będą gromadzone jako dane do analiz i raportów. Pomiary będą mogły być raportowane na żywo do Systemu w celu dalszej analizy oraz wykrywania anomalii w sieci w tym ataków oraz zagrożeń sieci operatorskiej oraz klienckiej. Wśród parametrów wchodzących w skład pomiarów wchodziły będą między innymi:

- pasmo łącza,
- latencja łącza,
- poziom dostępności usługi,
- Informacje na temat trasowania łącza,
- informacje dotyczące bezpieczeństwa łącza:
    - ataki DoS/DDoS,
    - ataki oraz uczestnictwo w botnetach,
    - ataki na protokoły trasowania (BGP, vlan spoofing oraz inne),
    - anomalia bezpieczeństwa sieci,
    - inne ataki na sieć PT oraz UK,
- kompromitacja sieci i urządzeń użytkownika:
    - uczestnictwo sieci oraz urządzeń w klastrach botnet,
    - połączenia z sieci użytkownika do szkodliwych sieci orz urządzeń, takich jak serwery Command-and-Control (C&C),
    - inne parametry bezpieczeństwa sieci oraz urządzeń,
- uczestnictwo w atakach typu „zombie”,
- połączenia z niebezpiecznymi sieciami oraz urządzeniami;
- inne parametry bezpieczeństwa sieci.

Urządzenia pomiarowe wytworzone w ramach Projektu dzielą się na 2 typy:

- próbniki konsumenckie – niewielkie urządzenia pomiarowe pozwalające na zamontowanie oraz analizę w sieci końcowej Użytkownika Końcowego, udostępniane przez UKE,

- próbniki sieciowe – urządzenia i aplikacje pomiarowe montowane na węzłach sieci PT, pozwalające na analizę łącza bezpośrednio w sieci operatorskiej. Charakteryzowały się one będą większą przepustowością oraz większymi możliwościami analizy dzięki brakowi ograniczeń takich jak wielkość urządzenia.

Próbniki zostaną certyfikowane przez niezależny podmiot certyfikujący pod względem kompatybilności, zgodności i jakości pomiarowej.

Dzięki korelacji wyników pomiędzy dwoma typami próbników, możliwe stanie się wykrywanie anomalii sieci takich jak:

- nadmierne obciążenie sieci w danym rejonie geograficznym;
- ataki na węzły sieciowe;
- ataki na systemy operatorskie;
- ataki na segmenty sieci w tym:
    - wybrane podsieci;
    - wybranych operatorów;
    - wybranych klientów;
    - wybrane lokalizacje.

Dodatkowo, próbniki będą mogły być przenoszone pomiędzy różnymi węzłami oraz sieciami klienckimi w celu poszerzenia zasięgu oraz elastyczności możliwości monitorowania sieci oraz jej segmentów.

System SMJI będzie agregował dane dotyczące jakości oraz bezpieczeństwa łączy UK oraz PT dzięki zastosowaniu sieci próbników wykonujących pomiary a w przypadku wykrycia luk bezpieczeństwa lub ataków na sieć, informacje zagregowane w ramach systemu SMJI będą mogły być przekazane do odpowiednich ISAC i CSIRT poziomu krajowego w celu reakcji oraz obsłużenia ryzyka.

W ramach E-Usługi, Zamawiający zwraca szczególną uwagę na **konieczność uproszczenia pozyskania z systemu informacji przez użytkownika końcowego** przy spełnieniu postulatów dostępności (łatwo znaleźć i zidentyfikować); zrozumiałości (czytelne, niezbyt techniczne); sensowności (istotne dla konsumentów); porównywalności (ujednolicona prezentacja) i dokładności (rzetelne i dokładne).

3. Przepisy i wymogi prawne

Potrzeba realizacji E-Usługi wynika z zapisów Ustawy PT oraz z planowanego wdrożenia ustawy Prawo komunikacji elektronicznej (PKE), która zastąpi Ustawę PT i będzie regulowała m.in. usługi IAS.

Celem zmian legislacyjnych jest m.in. wdrożenie dyrektywy PE i Rady (UE) 2018/1972 z 11.12.2018 ustanawiającej Europejski kodeks łączności elektronicznej (EKŁE), który zawiera przepisy regulujące sektor łączności elektronicznej, w tym usługi IAS. Cele EKŁE to m.in.: powstanie zrównoważonej konkurencji i korzyści dla użytkowników końcowych (UK); zapewnienie świadczenia publicznie dostępnych, przystępnych cenowo usług dobrej jakości.

Zgodnie z Art. 192 ust. 1 Ustawy PT, Prezes UKE jest organem regulacyjnym w dziedzinie rynku usług telekomunikacyjnych, w tym usług IAS.

Zgodnie z Art. 192 ust. 1 Ustawy PT do zakresu działania Prezesa UKE należy m.in.:

a. regulacja i kontrola rynków usług telekomunikacyjnych;

b. analiza i ocena funkcjonowania rynków usług telekomunikacyjnych;
c. podejmowanie interwencji oraz decyzji w sprawach dotyczących funkcjonowania rynku usług telekomunikacyjnych z własnej inicjatywy lub wniesionych przez zainteresowane podmioty, w szczególności użytkowników i przedsiębiorców telekomunikacyjnych;
d. realizacja obowiązków i kontrolowanie realizacji obowiązków wynikających z przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2015/2120[12];
e. rozstrzyganie sporów w zakresie właściwości Prezesa UKE;
f. przygotowanie i publikacja corocznych raportów o stanie rynku telekomunikacyjnego na podstawie informacji uzyskanych od przedsiębiorców telekomunikacyjnych oraz innych podmiotów dysponujących infrastrukturą telekomunikacyjną lub realizujących inwestycje w tym zakresie.

Przedmiotem zamówienia jest rozbudowany system, za pomocą którego zostanie udostępniona E-Usługa, czyli system pomiarów i gromadzenia informacji o jakości usług dostępu do Internetu. Tworzony system składać się będzie z wielu powiązanych elementów, które będą realizować poszczególne funkcjonalności. Poszczególne elementy systemu muszą gwarantować zgodność danych elementów z przepisami prawa oraz realizację danej funkcjonalności gwarantującą zgodność i bezpieczeństwo prawne.

Poszczególne elementy systemu, w tym komponenty hardware oraz wykorzystywane do realizacji projektu urządzenia pomiarowe mobilne i stacjonarne muszą spełniać wymagania prawne w zakresie dopuszczenia danych produktów do obrotu, wynikające między innymi z poniżej wskazanych aktów:

1. Dyrektywa Parlamentu Europejskiego i Rady 2014/53/UE z dnia 16 kwietnia 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących urządzeń radiowych i uchylająca dyrektywę 1999/5/WE (Dz. Urz. UE L 153 z dnia 22.05.2014, str. 62)
2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) 305/2011 (Dz. U. UE L 169 z dnia 25.06.2019, str. 1)
3. Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93 (Dz. U. UE L 218 z dnia 13.08.2010, str. 30)
4. Ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (t.j. Dz. U. z 2022 r. poz. 5 z późn. zm)
5. Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz. U. z 2021 r. poz. 576 z późn. zm.)
6. Rozporządzenie Ministra Cyfryzacji z dnia 17 czerwca 2016 r. w sprawie dokonywania oceny zgodności urządzeń radiowych z wymaganiami (Dz. U. z 2016 r. poz. 878)
7. Rozporządzenie Wykonawcze Komisji (UE) 2017/1354 z dnia 20 lipca 2017 r. określające sposób podawania informacji przewidzianych w art. 10 ust. 10 dyrektywy Parlamentu Europejskiego i Rady 2014/53/UE (Dz.U.L.2017.190.7.)

[12] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/2120 z dnia 25 listopada 2015 r. ustanawiające środki dotyczące dostępu do otwartego internetu oraz zmieniające dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, a także rozporządzenie (UE) nr 531/2012 w sprawie roamingu w publicznych sieciach łączności ruchomej wewnątrz Unii, Dz.U. L 310 z 26.11.2015, https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A32015R2120

8. Rozporządzenie Delegowane Komisji (UE) 2019/320 z dnia 12 grudnia 2018 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady 2014/53/UE w odniesieniu do stosowania zasadniczych wymagań, o których mowa w art. 3 ust. 3 lit. g) tej dyrektywy w celu zapewnienia możliwości ustalenia lokalizacji osób dokonujących zgłoszeń alarmowych za pomocą urządzeń przenośnych (Dz.U.L.2019.55.1.).
9. Dyrektywa Parlamentu Europejskiego i Rady 2014/30/UE z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do kompatybilności elektromagnetycznej (Dz. Urz. UE L 96 z 29.03.2014, str. 79)
10. Ustawa z dnia 30 sierpnia 2002 r. o systemie oceny zgodności (t.j. Dz. U. z 2021 r., poz. 1344 z późn. zm)
11. Rozporządzenie Ministra Gospodarki z dnia 17 grudnia 2010 r. w sprawie oceny zgodności wyrobów wykorzystujących energię oraz ich oznakowania (t.j. Dz. U. z 2022 r., poz. 599)
12. Rozporządzenie Komisji (WE) nr 1275/2008 z dnia 17 grudnia 2008 r. w sprawie wykonania dyrektywy 2005/32/WE Parlamentu Europejskiego i Rady w odniesieniu do wymogów dotyczących ekoprojektu dla zużycia energii przez elektryczne i elektroniczne urządzenia gospodarstwa domowego i urządzenia biurowe w trybie czuwania i wyłączenia oraz czuwania przy podłączeniu do sieci (Dz.U.UE.L.2008.339.45 ze zm.)
13. Rozporządzenie Komisji (WE) nr 107/2009 z dnia 4 lutego 2009 r. w sprawie wykonania dyrektywy 2005/32/WE Parlamentu Europejskiego i Rady w odniesieniu do wymogów dotyczących ekoprojektu dla prostych set-top boksów (Dz.U.UE.L.2009.36.8);
14. Rozporządzenie Komisji (WE) nr 278/2009 z dnia 6 kwietnia 2009 r. w sprawie wykonania dyrektywy 2005/32/WE Parlamentu Europejskiego i Rady w odniesieniu do wymogów dotyczących ekoprojektu w zakresie zużycia energii elektrycznej przez zasilacze zewnętrzne w stanie bez obciążenia oraz ich średniej sprawności podczas pracy (Dz.U.UE.L.2009.93.3);
15. Rozporządzenie Komisji (WE) nr 642/2009 z dnia 22 lipca 2009 r. w sprawie wykonania dyrektywy 2005/32/WE Parlamentu Europejskiego i Rady w odniesieniu do wymogów dotyczących ekoprojektu dla telewizorów (Dz.U.UE.L.2009.191.42)
16. Rozporządzenie Komisji (UE) nr 617/2013 z dnia 26 czerwca 2013 r. w sprawie wykonania dyrektywy Parlamentu Europejskiego i Rady 2009/125/WE w odniesieniu do wymogów dotyczących ekoprojektu dla komputerów i serwerów (Dz. Urz. UE L 175 z 27.06.2013 , str. 13)
17. Dyrektywa Parlamentu Europejskiego i Rady 2011/65/UE z dnia 8 czerwca 2011 r. w sprawie ograniczenia stosowania niektórych niebezpiecznych substancji w sprzęcie elektrycznym i elektronicznym (Dz.Urz.UE.L 2011 Nr 174, str. 88)
18. Rozporządzenie Ministra Rozwoju i Finansów z dnia 21 grudnia 2016 r. w sprawie zasadniczych wymagań dotyczących ograniczenia stosowania niektórych niebezpiecznych substancji w sprzęcie elektrycznym i elektronicznym (t.j. Dz. U. z 2021 r. poz. 1513 z późn. zm).

Poszczególne komponenty aplikacyjne (usługowo-pomiarowe) muszą gwarantować bezpieczeństwo przetwarzanych i gromadzonych danych, w szczególności w aspekcie tajemnicy telekomunikacyjnej jak również w aspekcie danych osobowych oraz bezpieczeństwa pozyskiwanych i gromadzonych danych.

System będzie miał dostęp / zarządzał szeregiem wrażliwych danych takich jak:

- Dane osobowe
- Dane o zachowaniu klientów usługi internet

- Dane o infrastrukturze technicznej przedsiębiorców

System musi gwarantować bezpieczeństwo wskazanych między innymi danych oraz gwarantować animizację w przypadku prezentacji wyników pomiarów.

Wykorzystywane w projekcie systemy powinny gwarantować zgodność z wymaganiami bezpieczeństwa systemów zawartych w:

1. ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2020 r. poz. 1369);
2. rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz.U. z 2017 r. poz. 2247);
3. uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (MP 2019.1037.1);
4. uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa" (MP 2019.862.1).
5. Narodowe Standardy Cyberbezpieczeństwa (NSC) w zakresie architektury bezpieczeństwa systemów teleinformatycznych w modelu „Zero zaufania" (NSC 800-207);
6. Narodowe Standardy Cyberbezpieczeństwa w zakresie przewodnika po telepracy w przedmiocie publicznym (NSC 800-46);
7. „Standardy Cyberbezpieczeństwa Chmur Obliczeniowych" opracowane w ramach zbioru Narodowych Standardów Cyberbezpieczeństwa.

W zakresie gromadzonych i przetwarzanych przez komponenty systemu danych osobowych całościowy system musi zapewniać zgodność z:

1. Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz.UE.L 2016 Nr 119, str. 1);
2. Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. 2019 poz. 1781 z późn. zm.);
3. Rozporządzeniem Ministra Cyfryzacji z dnia 10 marca 2020 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników (Dz.U. z 2020 r. poz. 399);
4. Ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących działania publiczne (t.j. Dz.U. z 2021 r. poz. 2070 z późn. zm.);
5. Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz.U. z 2017 r. poz. 2247);
6. Ustawą z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2020 r. poz. 344 z późn. zm.).

Wykonawca jest zobowiązany do monitorowania i analizy zmian w przepisach prawa mających wpływ na wymagania opisane dot. przedmiotu zamówienia.

Wykonawca jest zobowiązany do zapewnienia zgodności przedmiotu zamówienia z przepisami prawa obowiązującymi na terytorium Polski w dniu podpisania umowy (w tym takich, co do których wiadomo, że w dniu Odbioru Końcowego będą miały zastosowanie w przyszłości, np. znajdują się w okresie vacatio legis).

Wykonawca jest zobowiązany do zapewnienia zgodności przedmiotu zamówienia z przepisami prawa obowiązującymi na terytorium Polski w dniu przekazania przedmiotu zamówienia do Odbioru Końcowego.

4. Systemy istniejące

Projektowana e-usługa musi współpracować z istniejącymi wewnętrznymi systemami Zamawiającego jak i zewnętrznymi systemami dostarczanymi przez podmioty trzecie, wyszczególnionymi poniżej.

4.1. Wykaz systemów wewnętrznych Zamawiającego

1. PIT - Punkt Informacyjny ds. Telekomunikacji (PIT) dla terytorium Rzeczpospolitej Polskiej został utworzony w związku z implementacją w Polskim prawie postanowień dyrektywy Parlamentu Europejskiego i Rady, nr 2014/61/UE z dnia 15 maja 2014 r. w sprawie środków mających na celu zmniejszenie kosztów realizacji szybkich sieci łączności elektronicznej. Został zintegrowany z Platformą Usług Elektronicznych UKE (PUE) oraz z Profilem Zaufanym (PZ). PIT umożliwia przedsiębiorcom telekomunikacyjnym dostęp do posiadanych przez Prezesa UKE informacji o:
   a. formalnoprawnej stronie realizacji inwestycji telekomunikacyjnych,
   b. aktualnym stanie infrastruktury i jej lokalizacji,
   c. warunkach dostępu do infrastruktury.

   PIT to jedno miejsce informacyjne o zasadach i warunkach inwestowania oraz o istniejących i planowanych zasobach.

   Docelowo PIT udzieli inwestorom wszystkich niezbędnych informacji o formalno-prawnej stronie realizowania inwestycji, dostarczy kompletnych informacji o aktualnym stanie infrastruktury technicznej, planach jej dotyczących i lokalizacji.

   Więcej informacji pod adresem: https://pit.uke.gov.pl/plpl/o-projekcie
2. ASDI - Atlas Szerokopasmowego Dostępu do Internetu. Atlas służy do gromadzenia, przetwarzania, prezentowania i udostępniania informacji o:
   a. infrastrukturze telekomunikacyjnej (w tym informacje o wartościach przepływności poszczególnych łączy),
   b. publicznych sieciach telekomunikacyjnych,
   c. budynkach umożliwiających kolokację.

   Dane te służą UKE do sporządzania, weryfikowania i aktualizacji inwentaryzacji, o której mowa w art. 29 ust.1 ustawy o wspieraniu rozwoju usług i sieci i raportowania ich m.in. do Komisji Europejskiej. Informacje są udostępniane przedsiębiorcom, jednostkom samorządu terytorialnego, administracji i obywatelom.

   Więcej informacji pod adresem: https://mapbook.uke.gov.pl
3. RJST - Rejestr Jednostek Samorządu Terytorialnego - Rejestr Jednostek Samorządu Terytorialnego (RJST) wykonujących działalność w zakresie telekomunikacji wraz z zakresem świadczonych usług. Te Informacje są dostępne dla przedsiębiorców, jednostek samorządu terytorialnego, administracji oraz obywateli.

Więcej informacji pod adresem: https://bip.uke.gov.pl/rjst/

4. RPT - Rejestr Przedsiębiorców Telekomunikacyjnych. Rejestr Przedsiębiorców Telekomunikacyjnych wraz z zakresem świadczonych usług. Te informacje są dostępne dla przedsiębiorców, jednostek samorządu terytorialnego, administracji oraz obywateli.

   Więcej informacji pod adresem: https://bip.uke.gov.pl/rpt/

5. KiE - Kontrola i Egzekucja Wykonania Obowiązków Operatorów. Zasoby administracyjno- kontrolne Prezesa UKE co do wykonywania obowiązków przedsiębiorców telekomunikacyjnych wobec prawa krajowego i UE.

   Więcej informacji pod adresem: https://www.uke.gov.pl/o-nas/departamenty-i-biura/#departamentkontroli

6. CIK – Centrum Informacji Konsumenckiej - Strona internetowa skierowana bezpośrednio do konsumentów, użytkowników usług telekomunikacyjnych. Strona internetowa wchodzi w skład Centrum Informacji Konsumenckiej, w ramach którego działa również infolinia konsumencka. Na infolinii eksperci UKE udzielają porad konsumentów oraz podejmują również interwencje w sprawach dotyczących funkcjonowania rynku usług telekomunikacyjnych i pocztowych. CIK prowadzi także kampanie informacyjno-edukacyjne dla użytkowników rynków telekomunikacyjnego i pocztowego.

   Więcej informacji pod adresem: https://cik.uke.gov.pl

7. AD – Active Directory - Usługa katalogowa (hierarchiczna baza danych) dla systemów Windows będąca implementacją protokołu LDAP, zapewniająca uwierzytelnienie obiektów (użytkowników wewnętrznych, komputerów) i autoryzację (bądź jej odmowę) do innych zasobów UKE. Niezbędna jest integracja projektowanej e-usługi z powyższym rozwiązaniem.
8. WSO2IS/CSU - Centralny System Uwierzytelnienia oparty na rozwiązaniu WSO2 Identity Server, który realizuje technikę pojedynczego logowania (z ang. Single Sign On) do wielu aplikacji. Wykorzystywany u Zamawiającego w celu uwierzytelniania użytkowników wewnętrznych jak i klientów zewnętrznych do systemów i usług. Niezbędna jest integracja projektowanej e-usługi z powyższym rozwiązaniem.

4.2. Wykaz systemów zewnętrznych:

1. Portal Web - Mapping of Broadband Services in Europe, EC - Interaktywna platforma map, pokazująca jakość Internetu dostarczanego przez sieci szerokopasmowe w całej Europie. Europejska mapa szerokopasmowa daje decydentom politycznym, a także prywatnym inwestorom możliwość monitorowania postępów we wdrażaniu sieci o dużej przepustowości i jakości usług szerokopasmowych w Europie. Możliwość publikacji własnych zbiorów danych.

   Więcej informacji pod adresem: https://www.broadbandmapping.eu/

2. KWIE - Krajowy Węzeł Identyfikacji Elektronicznej - To prosty i bezpieczny dostęp do usług publicznych online. Pozwala używać uniwersalnego loginu i bezpiecznego hasła oraz korzystać z różnych środków identyfikacji elektronicznej w dostępie do różnych serwisów i usług w Internecie.

   Więcej informacji pod adresem: https://login.gov.pl

3. Geoportal – Strona geoportal.gov.pl pełni rolę centralnego węzła Infrastruktury Informacji Przestrzennej pośrednicząc w dostępie do danych przestrzennych i związanych z nimi usług. Dane centralnego zasobu geodezyjnego i kartograficznego:
   a. Osnowy geodezyjne, grawimetryczne i magnetyczne,

b. Państwowy rejestr granic i jednostek podziałów terytorialnych kraju,
c. Ortofotomapa,
d. Mapy topograficzne,
e. Państwowy Rejestr Nazw Geograficznych,
f. Dane pomiarowe,
g. Numeryczny model terenu,
h. Numeryczny model pokrycia terenu,
i. Mapy tematyczne,
j. Baza Danych Obiektów Ogólnogeograficznych,
k. Zintegrowane kopie baz danych obiektów topograficznych BDOT10k,
l. Zobrazowania lotnicze.

Więcej informacji pod adresem: https://geoportal.gov.pl

4. Dane.gov.pl - Portal danych jako źródło wiarygodnych, na bieżąco aktualizowanych danych, udostępnianych bezpłatnie do ponownego wykorzystywania, pochodzących z administracji publicznej oraz podmiotów prywatnych. Portal stworzony z myślą o:
   a. obywatelach zainteresowanych działaniami państwa,
   b. firmach, które budują innowacyjne produkty i usługi oparte na danych,
   c. organizacjach pozarządowych, wykorzystujących dane w codziennej pracy,
   d. naukowcach prowadzących badania,
   e. urzędnikach przygotowujących raporty i analizy.

   Więcej informacji pod adresem: https://dane.gov.pl
5. PST - Pro Speed Test - Certyfikowany Mechanizm Monitorowania Jakości usługi dostępu do Internetu zwany „PRO Speed Test" stworzony na podstawie umowy UKE z komercyjną firmą VSpeed sp. z o.o. Wyniki pomiarów zrealizowanych w określonych warunkach mogą być m.in. podstawą dochodzenia roszczeń w procesie reklamacyjnym pomiędzy użytkownikami i dostawcami usługi.

   Więcej informacji pod adresem: https://pro.speedtest.pl oraz https://cik.uke.gov.pl/uslugi-teleko/pomiar-predkosci-internetu/certyfikowany-mechanizm/

4.3. Przepływy pomiędzy systemami

Poniższa tabela ukazuje powiązania i przepływy pomiędzy systemami już istniejącymi a projektowaną e-usługą:

Tabela 3 - Przepływy i powiązania pomiędzy systemami

LP.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
1	PIT	SMJI	Dane o stanie realizacji inwestycji telekomunikacyjnych, aktualnych zasobach infrastruktury i jej lokalizacji, warunkach dostępu do infrastruktury.	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych: - przez Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych: - przez Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych - standard API
2	SMJI	PIT	Statystyki z pomiarów SMJI w sieciach przedsiębiorców (operatorów, dostawców usług) z ich prezentacją w różnych przekrojach, obszarach i okresach na obszarze całego kraju lub wybranych regionach będą bezpłatnie dostępne dla użytkowników indywidualnych, biznesowych i przedsiębiorców.	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych: - przez Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych - standard API

LP.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
3	SMJI	Atlas Szerokopasmowego Dostępu do Internetu - ASDI	Dane techniczne i geograficzne o wartościach przepływności poszczególnych łączy Internetowych, publicznych sieciach telekomunikacyjnych oraz o zakończeniach łączy na poziomie budynku umożliwiających kolokację.	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych - przez Tryb odwołań bezpośrednich (13 ust. 2) KRI	Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych – usługa WMS/WMTS
4	Rejestr Jednostek Samorządu Terytorialnego - RJST	SMJI	Dane o prowadzonej działalności telekomunikacyjnej na poziomie samorządów lokalnych w zakresie infrastruktury i zakresie świadczonych usług.	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych:- przez Tryb odwołań bezpośrednich(§13 ust. 2) KRI	Tryb odwołań bezpośrednich(§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych – standard WebDAV (wymiana danych zapisanych w formacie csv)
5	Kontrola i Egzekucja Wykonania Obowiązków Operatorów - KiE	SMJI	Dane z wykonywanych postępowań kontrolnoadministracyjnych Prezesa UKE wobec przedsiębiorców telekomunikacyjnych.	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych:- przez Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych – możliwość pobierania danych statystycznych z ESOD bądź Hurtowni Danych.

LP.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
6	SMJI	Kontrola i Egzekucja Wykonania Obowiązków Operatorów - KiE	Dane z wykonywanych postępowań kontrolno-administracyjnych Prezesa UKE wobec przedsiębiorców telekomunikacyjnych.	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych: - przez Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych - standard HTTPS
7	SMJI	Centrum Informacji Konsumenckiej - CIK	Dane od osób zainteresowanych, klientów CIK - skargi, uwagi, wnioski dotyczące telekomunikacji (usług, infrastruktury, obrotu urządzeniami).	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych: - przez Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych - standard HTTPS
8	RPT	SMJI	Dane o Przedsiębiorcach Telekomunikacyjnych w kraju wraz z zakresem i parametrach świadczonych przez nich usług.	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych: - przez Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych - standard WebDAV (wymiana danych zapisanych w formacie csv)
9	WSO2IS/CSU	SMJI	adres e-mail, hasło, imię , nazwisko, PESEL	Inicjowany przez Klienta za pośrednictwem web interfejsu - adresu email	Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych - standard HTTPS

LP.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
10	SMJI	WSO2IS/CSU	adres e-mail, hasło, imię , nazwisko, PESEL	Inicjowany przez Klienta za pośrednictwem web interfejsu - adresu email	Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych - standard HTTPS
11	PIT	WSO2IS/CSU	adres e-mail, hasło, imię , nazwisko, PESEL	Inicjowany przez Klienta za pośrednictwem web interfejsu - adresu email	Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych - standard HTTPS
12	WSO2IS/CSU	PIT	adres e-mail, hasło, imię , nazwisko, PESEL	Inicjowany przez Klienta za pośrednictwem web interfejsu - adresu email	Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych - standard HTTPS
13	Active Directory (AD)	SMJI	Udostępnienie tożsamości AD pozwalającej na logowanie do systemu wszystkich użytkowników wewnętrznych UKE.	Inicjowany przez pracownika UKE za pomocą klienta AD	Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych
14	SMJI	Active Directory (AD)	Udostępnienie tożsamości AD pozwalającej na logowanie do systemu wszystkich użytkowników wewnętrznych UKE.	Inicjowany przez pracownika UKE za pomocą klienta AD	Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych

LP.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
15	PRO Speed Test	SMJI	Dane o wynikach pomiarów zrealizowanych przez klientów usług w celu reklamacji składanym dostawcom usługi IAS.	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych: - przez Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych - standard HTTPS
16	GEO-PORTAL	SMJI	Ortofotomapa, Mapy topograficzne, Państwowy Rejestr Nazw Geograficznych i Dane pomiarowe, Numeryczny model terenu, Numeryczny model pokrycia terenu.	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych: przez Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych - standard HTTPS
17	SMJI	system dane.gov.pl	Prezentacja raportów z projektowanej e-usługi cyfrowej.	Automatyczny dla raportów okresowych lub inicjowany przez pracownika UKE z wykorzystaniem udostępnionych mechanizmów(API)	Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych - standard HTTPS

LP.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
18	Krajowy Węzeł Identyfikacji Elektronicznej	SMJI	W przypadku udanego uwierzytelnienia - przekazanie, w bezpieczny sposób, do systemu DU zestawu danych takiegoż użytkownika (numer identyfikacyjny, imię, nazwisko, nazwisko panieńskie, data urodzenia, miejsce urodzenia, płeć, adres +dodatkowe dane techniczne).	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych: - przez Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych - standard HTTPS, oraz SOAP i REST

LP.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
19	SMJI	Portal Web Komisji UE (EC)*)	Dane od Regulatorów krajów UE. Pochodzą z obliczeń teoretycznych i pomiarów. Obejmują 3 kategorie danych dla „Quality of Service" (QoS): - QoS-1: Obliczona dostępność usługi - teoretyczne obliczenia zasięgu przez operatorów sieci - QoS-2: Mierzone świadczenie usług - pomiary za pomocą sond panelowych lub testów dysków, bez uwzględnienia środowiska użytkownika końcowego - QoS-3: Mierzone doświadczenie usługi - pomiary za pomocą testów prędkości online, w tym środowisko użytkownika końcowego / rzeczywiste doświadczenia.	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych: - przez Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych - standard HTTPS

*) Portal Web Komisji UE (EC) - Mapowanie usług szerokopasmowych w UE (Mapping of Broadband Services in Europe, EC, w tym w zakresie e- usługi czyli dostępu do informacji o jakości usług IAS (Internet Access Service)

5. Harmonogram realizacji zamówienia

LATA	2022							2023										
MIESIĄCE	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11
Opracowane systemu SMJI od strony programistycznej, sprzętowej oraz dokumentacyjnej.																		
Przeprowadzenie I fazy testów akceptacyjnych systemu SMJI w modelu laboratoryjnym (symulacyjnym) oraz optymalizacja systemu SMJI po testach.																		
Przeprowadzenie II fazy testów akceptacyjnych systemu SMJI w modelu eksploatacyjnym (instalacja sprzętu w jednym punkcie wymiany ruchu międzyoperatorskiego oraz u 8 wybranych przedsiębiorców telekomunikacyjnych) oraz optymalizacja systemu SMJI po testach.																		
Przeprowadzenie III fazy testów akceptacyjnych systemu SMJI w warunkach rzeczywistych (instalacja wszystkich komponentów sprzętowo-programowych w dwóch EXP i u 20 przedsiębiorców telekomunikacyjnych na terenie całej Polski) oraz optymalizacja systemu SMJI po testach.																		
Odbiór końcowy Systemu e-usługi przez Zamawiającego (komponentów sprzętowych, komponentów programowych, dokumentacji powykonawczej, kodów źródłowych, bibliotek, praw autorskich, licencji standardowego oprogramowania) oraz rozpoczęcie świadczeń gwarancyjnych.																		

6. Wymagania w zakresie E-Usługi

EUs-1. Zamawiający wymaga aby wdrożona w ramach niniejszego zamówienia E-Usługa umożliwiała pełną (od wszczęcia do zakończenia), realizowaną w całości elektronicznie obsługę spraw dotyczących zapytań, wniosków i interwencji w przedmiocie jakości usług IAS:

a. dla PT (typ A2B) co najmniej w zakresie:
   i. sprawozdawania Prezesowi UKE informacji o deklarowanych i faktycznych wskaźnikach jakości usług IAS;
   ii. ustalenia i weryfikacji parametrów technicznych i jakościowych łącza współdzielonego;
   iii. dostępu do bieżącej informacji o jakości usług IAS;
   iv. pozyskania certyfikowanego przez Prezesa UKE raportu o faktycznych wskaźnikach jakości usług IAS (w tym też dla łącza współdzielonego);
   v. porównania faktycznych wskaźników jakości usług IAS podmiotów konkurencyjnych;
   vi. dostępu do informacji oraz zdarzeń dotyczących bezpieczeństwa PT oraz sieci UK.
b. dla UK (typ A2C) co najmniej w zakresie:
   i. dostępu do bieżącej informacji o jakości usług IAS;
   ii. ustalenia faktycznych wskaźników jakości posiadanej usługi IAS w celu porównania z wartościami deklarowanymi w ofercie, regulaminie, umowie;
   iii. porównania faktycznych wskaźników jakości usług IAS dostarczanych w budynku, dzielnicy, najbliższej okolicy (np. przy ulicy) w celu wyboru optymalnej oferty lub zmiany obecnego dostawcy;
   iv. pozyskania certyfikowanego przez Prezesa UKE raportu o faktycznych wskaźnikach jakości usług IAS;
   v. dostępu do informacji oraz zdarzeń dotyczących bezpieczeństwa PT oraz sieci UK.

EUs-2. E-Usługa spełnia co najmniej wymagania dla usługi publicznej udostępnionej on-line o stopniu dojrzałości 3 – dwustronna interakcja, dla której konieczne jest[13]:

a. udostępnienie na publicznie dostępnej stronie internetowej formularzy do wypełnienia,
b. zapewnienie uwierzytelnienia w systemie teleinformatycznym obywatela lub przedsiębiorcy,
c. umożliwienie wszczęcia sprawy (usługi) drogą elektroniczną rozumiane jako złożenie wniosku w postaci elektronicznej wraz z wymaganymi załącznikami.

EUs-3. E-Usługa umożliwia transfer danych w dwóch kierunkach: od usługodawcy (PT) do klienta (UK) oraz od klienta do usługodawcy.

EUs-4. UK i PT mogą pobierać z wykorzystaniem E-Usługi informacje o jakości usług IAS w celach informacyjnych (pomiar niecertyfikowany) lub jako materiał o odpowiedniej mocy dowodowej (pomiar certyfikowany) w celu dochodzenia swoich roszczeń.

[13] Poradnik *Standard opisu elektronicznej usługi publicznej w działaniu 2.1 POPC*, Rozdział 6. Pojęcie dojrzałości e-usługi publicznej, Praktyczne poradniki, POPC Wsparcie, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/popcwsparcie/praktyczne-poradniki

EUs-5. E-usługa pozwoli na ponowne wykorzystanie danych zebranych podczas kolejnych sesji pomiarowych, w wyniku czego można będzie śledzić zmianę jakości usługi IAS w czasie oraz wskazać trendy w regionie lub w ramach sieci wskazanego Przedsiębiorcy Telekomunikacyjnego.

EUs-6. UK lub PT mogą otrzymywać informacje o bezpieczeństwie sieci, w tym alerty czasu rzeczywistego dotyczące występujących ataków oraz zagrożeń bezpieczeństwa w sieci.

EUs-7. E-Usługa zapewnia dostęp do rzetelnych i aktualnych informacji o usługach IAS prezentowanych w sposób przejrzysty i zrozumiały dla każdej grupy docelowej użytkowników: UK, PT, UKE.

EUs-8. E-Usługa zapewnia dostęp do niezaprzeczalnych informacji o faktycznej jakości świadczonych usług IAS o odpowiedniej mocy dowodowej (w przypadku postępowania reklamacyjnego, przed Prezesem UKE lub sądem).

EUs-9. E-Usługa zapewnia dostęp do informacji na temat jakości publicznie dostępnych usług IAS poszczególnych PT w testowanej lokalizacji.

EUs-10. E-Usługa daje możliwość poinformowania oraz zareklamowania niezgodności parametrów dostarczanej usługi z deklarowanymi w trybie ADR, oraz udzielenia odpowiedzi zwrotnej przez PT do UK.

EUs-11. E-Usługa daje możliwość zgłoszenia do UKE niezgodności parametrów usługi z deklarowanymi przez PT oraz udostępnienia UK informacji o wyniku analizy zgłoszenia.

EUs-12. E-Usługa zapewnia UK prezentację zagregowanej, bieżącej liczby zgłoszeń we wskazanej lokalizacji w podziale na miejscowość, gminę, powiat, województwo.

EUs-13. E-Usługa obejmuje serwis internetowy wraz z aplikacjami:

a. Obsługującymi pomiary i proces ich certyfikacji dla użytkownika końcowego – konsumenta w ramach indywidualnego, uwierzytelnionego konta.
b. Obsługującymi pomiary i proces ich agregowania w postaci raportów dla przedsiębiorców telekomunikacyjnych w ramach indywidualnego, uwierzytelnionego konta z dostępem dla uprawnionych, uwierzytelnionych użytkowników.
c. Obsługującymi procesy certyfikacji, postępowań ADR i interwencji u Zamawiającego w ramach zamodelowanych ról i uprawnień dla uwierzytelnionych kont użytkowników Zamawiającego.

EUs-14. Aplikacje E-Usługi umożliwiają w szczególności:

a. Eksplorację danych,
b. Analizy statystyczne,
c. Raportowanie,
d. Wizualizację wyników pomiarów

Za pomocą graficznego interfejsu użytkownika, umożliwiającego wykorzystanie funkcji mapy interaktywnej.

EUs-15. Podstawą działania E-Usługi w zakresie dostarczania i przetwarzania danych pomiarowych jest System Monitorowania Jakości Internetu (SMJI).

EUs-16. Aplikacje pomiarowe E-Usługi realizowane będą za pomocą SMJI poprzez typowe, używane na rynku urządzenia IT (stacjonarne i mobilne) oraz specjalistyczne próbniki pomiarowe zainstalowane w sieci Internet na terenie całego kraju. Dane i wyniki wszystkich powszechnie

prowadzonych pomiarów będą gromadzone w centralnej bazie danych obsługiwanej w systemie 24h/7d.

EUs-17. E-Usługa dostępna jest i zapewnia odpowiednie interfejsy dla:

a. Użytkownika końcowego – UK (typ A2C);

b. Przedsiębiorców telekomunikacyjnych – PT (typ A2B);

c. Personelu UKE.

EUs-18. E-Usługa udostępnia bazę danych obejmującą m.in. wyniki pomiarów historycznych i statystyki z pomiarów SMJI w sieciach wybranych PT z ich prezentacją w różnych przekrojach, obszarach i okresach na obszarze całego kraju lub wybranych regionach Rzeczypospolitej Polskiej, zgodnie z podziałem administracyjnym kraju.

EUs-19. E-usługa pozwala także na ponowne wykorzystanie danych zebranych podczas kolejnych sesji pomiarowych, w wyniku czego można będzie śledzić zmianę jakości usługi IAS w czasie oraz wskazać trendy w danym regionie lub w ramach sieci wskazanego PT.

EUs-20. E-usługa wprowadza element bezpieczeństwa dla Użytkowników Końcowych poprzez monitorowanie usług pod kątem możliwego, niekorzystnego oddziaływania na bezpieczeństwo obywatela, gospodarkę za pośrednictwem cyfrowych usług oferowanych przez przedsiębiorców za pośrednictwem PT.

EUs-21. E-Usługa udostępnia urządzenia i aplikacje pomiarowe dla PT (próbniki sieciowe) oraz Użytkowników Końcowych (próbniki konsumenckie), umożliwiające pomiary jakościowe oraz ilościowe, w tym obiektywne oraz certyfikowane pomiary parametrów łącza a także analizę bezpieczeństwa łącza.

EUs-22. Wymiana informacji pomiędzy e-usługami wchodzącymi w skład Projektu zostanie zabezpieczona odpowiednimi mechanizmami, np. certyfikatami klucza publicznego czy unikalnymi kluczami dostępowymi.

EUs-23. Informacja o E-Usłudze i odwołanie (możliwość zainicjowania transakcji) jest dostępna w ramach platformy ePUAP, serwisach internetowych Urzędu Komunikacji Elektronicznej, serwisie Obywatel.gov.pl, Biznes.gov.pl.

EUs-24. W zakresie interfejsu graficznego użytkownika, zastosowanie mają wymagania określone w rozdziale 7.8.

6.1. Szczególne funkcjonalności E-Usługi

Na etapie formułowania wymagań, Zamawiający zidentyfikował szczególne wymagania funkcjonalne dla E-Usługi:

WFE-1. Uzyskanie informacji o prawidłowym podłączeniu próbnika lub informacji o warunkach, które nie zostały spełnione dla prawidłowego podłączenia próbnika wraz ze wskazówkami.

WFE-2. UK i PT mogą monitorować proces pomiaru, mają bieżący dostęp do wyników pomiaru.

WFE-3. E-Usługa zapewnia prezentację bieżących i historycznych danych pomiarowych i stanów cyklów pomiarowych.

WFE-4. Powiadomienie o pomyślnym zakończeniu procesu pomiaru, ewentualnych problemach, dostępności certyfikatu pomiaru zarówno w interfejsie graficznym użytkownika jak i wg ustawionych przez użytkownika preferencji:

a. ePUAP,

b. e-mail,

c. SMS.

WFE-5. Możliwość pobrania uzyskanego certyfikatu pomiaru tylko po dokonaniu zwrotu próbnika konsumenckiego.

WFE-6. Informowanie użytkownika o powodach braku certyfikacji dla pomiaru.

WFE-7. Odniesienie do parametrów łącza IAS wynikających z umowy.

WFE-8. Prezentacja szczegółowych informacji na temat jakości usługi dostarczanej przez operatorów IAS – w tym danych historycznych.

WFE-9. Dostęp do historycznych, w tym archiwalnych informacji dotyczących pomiarów wraz z agregowaniem danych pod kątem:

a. daty i czasu z dokładnością do minut;

b. dostawcy IAS;

c. rejonu geograficznego zgodnie z podziałem administracyjnym kraju z dokładnością do miejscowości;

d. wyników pomiarów.

WFE-10. Wizualizacja danych w postaci wykresów i map.

WFE-11. Możliwość złożenia automatycznego postępowania reklamacyjnego ADR, popartego certyfikowanym oraz szeroko akceptowanym wynikiem pomiarowym.

WFE-12. Możliwość przeprowadzania testów ciągłych, dających informacje na temat bezpieczeństwa łącza w czasie.

WFE-13. Możliwość identyfikowania oraz raportowania w trybie 24/7, ataków oraz zagrożeń związanych z bezpieczeństwem sieci operatorskiej a także sieci Użytkowników Końcowych.

6.2. Zasoby danych o charakterze rejestru publicznego

Wdrożona E-Usługa udostępnia rejestr publiczny o dostępności i jakości świadczonych przez PT usług IAS. Szczególne wymagania względem rejestru:

WRP-1. Gromadzenie wiarygodnych, rzetelnych, porównywalnych, aktualnych oraz zrozumiałych informacji o jakości publicznie dostępnych usług IAS w oparciu o deklarowane przez PT parametry łączy i usług.

WRP-2. Porównanie wartości deklarowanych z wartościami zmierzonymi. Wyniki pomiaru jakości usług (QoS), w skali sieci krajowej; prezentacja statystyk danych zagregowanych w dostępie wg określonych profili (limity wskaźników, obszary geograficzne, typy i technologie usług, operatorzy, inne zidentyfikowane na etapie Analizy Przedwdrożeniowej).

WRP-3. Udostępnienie informacji dla przedsiębiorców telekomunikacyjnych związanych z wypełnieniem przez nich obowiązków zapewnienia przejrzystości i porównywalności informacji o dostępności i jakości usług IAS oferowanych i innych obowiązków QoS wynikających z prawa, z zastosowaniem interaktywnego mapowania i wizualizacji danych oraz aktywnych aplikacji *dashboard*.

WRP-4. Dostęp użytkownika końcowego do przejrzystej, rzetelnej i porównywalnej informacji o jakości usług IAS, pozwalającej na świadomy wybór dostawcy tych usług (spośród dających się porównać konkurencyjnych ofert) lub na przeprowadzenie autodiagnozy faktycznych wartości wskaźników jakości usługi IAS. W przypadku stwierdzenia rozbieżności pomiędzy deklarowanymi w ofercie lub informacji handlowej a faktycznymi wartościami wskaźników

jakości usług IAS, E-Usługa pozwoli użytkownikowi końcowemu na podjęcie postępowania reklamacyjnego wobec przedsiębiorcy telekomunikacyjnego.

WRP-5. Zgromadzone dane będą udostępniane przy użyciu publicznego API, umożliwiającego wymianę danych w sposób zautomatyzowany, oraz w sposób zapewniający integralność danych.

7. Wymagania w zakresie Systemu

WS-1. System będzie zarządzany i obsługiwany przez UKE.

WS-2. Pomiary będą odbywać się zgodnie z przyjętą metodą, w sposób zautomatyzowany, bez ograniczeń czasowych co oznacza, iż mogą rozpocząć się i zakończyć o dowolnej porze dnia a proces pomiarowy włącznie z przetwarzaniem i gromadzeniem danych musi być obsługiwany przez System w trybie ciągłym 24 godziny na dobę przez 7 dni w tygodniu.

WS-3. System dokonuje automatycznej analizy czynników środowiska pomiarowego, mających wpływ na jakość i możliwość przeprowadzenia pomiarów.

WS-4. Wyniki pomiarów będą gromadzone w Systemie jako dane źródłowe na potrzeby E-Usługi oraz do analiz i raportów przygotowywanych przez Zamawiającego.

WS-5. Dane i wyniki wszystkich powszechnie prowadzonych pomiarów (ze strony UKE, PT i przez użytkowników IAS) będą gromadzone w centralnej bazie danych obsługiwanej w systemie ciągłym (24h/7d).

WS-6. System będzie przygotowany na pracę w reżimie Big Data, tj. automatycznego generowania i gromadzenia danych nieosobowych bez bezpośredniej interwencji człowieka w ilościach masowych.

WS-7. System umożliwia identyfikowanie, raportowanie oraz wymianę informacji z zakresu bezpieczeństwa sieci, w tym raportowanie oraz wymianę danych z odpowiednimi ISAC i CSIRT poziomu krajowego.

WS-8. Baza danych Systemu obejmuje co najmniej wyniki pomiarów historycznych i statystyki z pomiarów SMJI w sieciach wybranych PT z ich prezentacją w różnych przekrojach, obszarach i okresach na obszarze kraju lub wybranych regionach.

WS-9. System udostępnia własne API (interfejs programistyczny aplikacji), pozwalający na automatyczną wymianę danych z systemami zewnętrznymi.

WS-10. Zamawiający przejmuje autorskie prawa majątkowe do kodów źródłowych Systemu.

WS-11. System będzie mógł być wykorzystywany przez inne organy administracji państwowej. Za pośrednictwem API i dedykowanych aplikacji możliwe będzie dokonywanie pomiarów usług IAS i weryfikacja ich z deklarowanymi przez dostawcę usługi parametrami oraz pod kątem bezpieczeństwa sieci. Proces uruchomienia komponentu pomiarowego odbywać się będzie w trybie roboczym na wniosek zainteresowanej strony a także w trybie ciągłym w sieciach operatorów usług IAS.

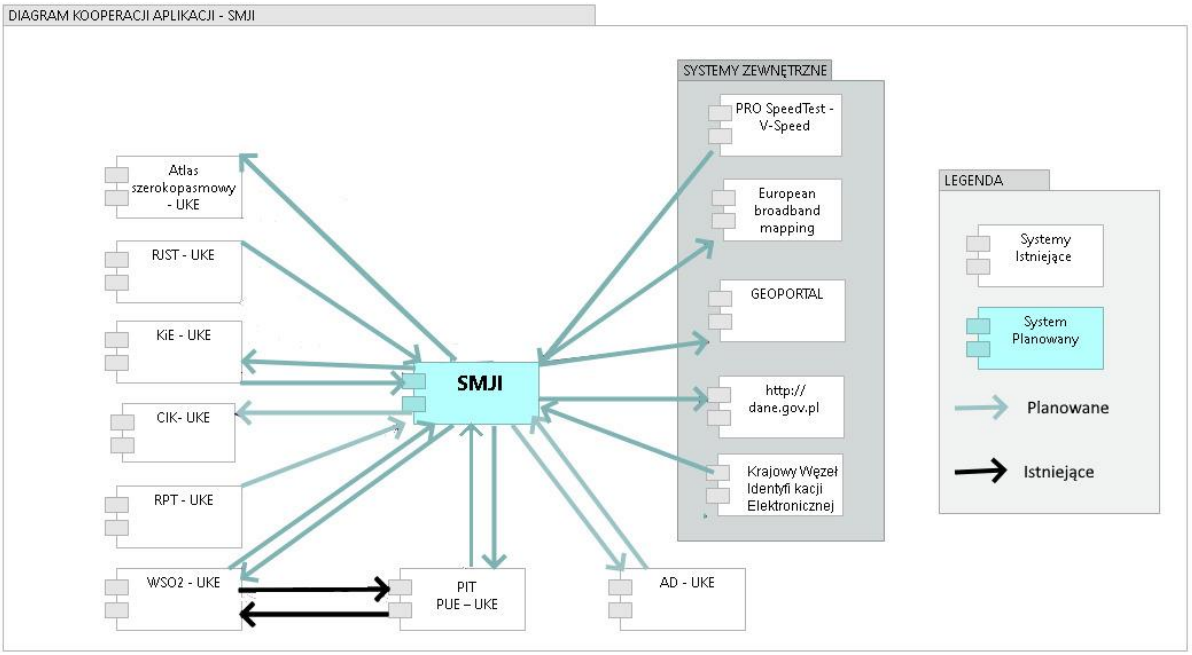
WS-12. System zapewni interoperacyjność zgodnie z zapisami w KRI (Krajowych Ram Interoperacyjności) oraz przyjętymi wytycznymi do konfiguracji usługi.

WS-13. System daje możliwość agregowania oraz przekazywania danych dotyczących bezpieczeństwa sieci, w tym przekazywania danych bezpieczeństwa do odpowiednich ISAC oraz CSIRT poziomu krajowego.

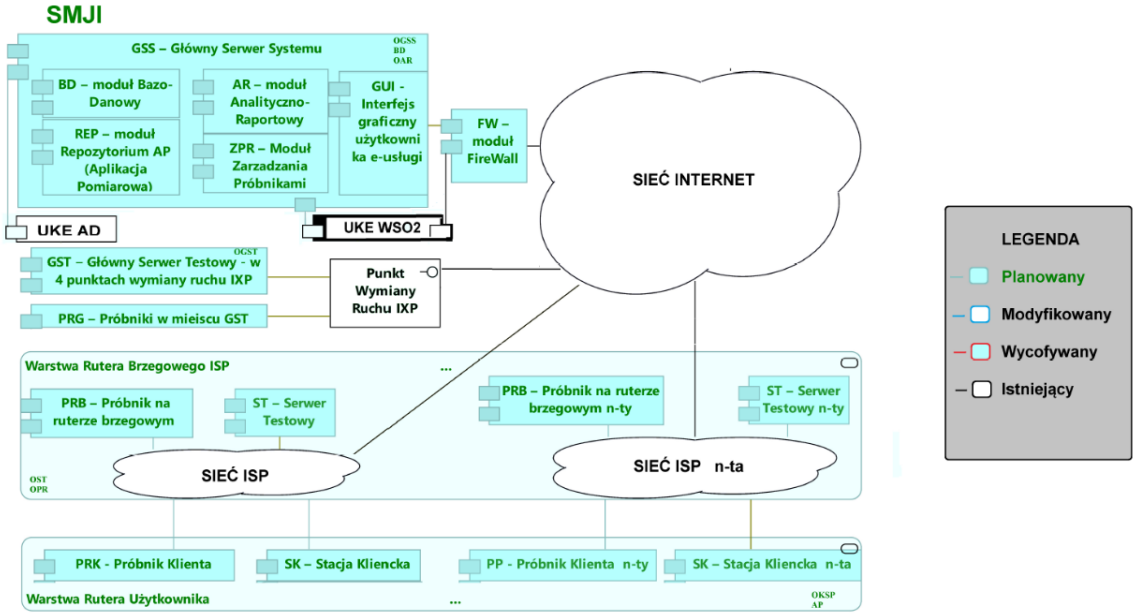
WS-14. System daje możliwość korelacji danych w tym danych bezpieczeństwa sieci z podziałem na charakterystyki takie jak: przedział czasu, rejon, operator IAS.

WS-15. Wykonanie systemu SMJI i E-Usługi powinno być realizowane z naciskiem na maksymalizację wykorzystania istniejących systemów jak Krajowy Węzeł Identyfikacji, Geoportal oraz możliwość przekazywania istotnych danych do systemu S46.

7.1. Wymagania w zakresie architektury Systemu



Rysunek 3 - Diagram kooperacji systemu SMJI



Rysunek 4 - Kluczowe komponenty architektury SMJI

Architektura Systemu musi uwzględniać pryncypia architektoniczne określone przez Radę Architektury Informacyjnej Państwa[14].

System zostanie zaprojektowany w architekturze mikroserwisów gdzie każdy z nich będzie osobnym kontenerem.

Do zarządzania zestawem kontenerów uruchomionych w klastrze maszyn wirtualnych wykorzystywany będzie dedykowany system wprowadzający automatyzację i orkiestrację (np. Kubernetes).

[14] Pryncypia architektoniczne, Portal Interoperacyjności i Architektury, Serwis Rzeczypospolitej Polskiej, https://www.gov.pl/web/ia/pryncypia-architektoniczne

7.2. Wymagania w zakresie technologii Systemu

Tabela 4 - Przyjęte założenia technologiczne dla SMJI

Lp.	Obszar	Założenie technologiczne
1.	Infrastruktura	1. System rozproszony w architekturze typu klient-serwer z możliwością logowania z wykorzystaniem mechanizmów: a. Krajowy Węzeł Identyfikacji Elektronicznej - login.gov.pl b. WSO2IS/CSU - dla użytkowników zewnętrznych, w przypadku braku możliwości zalogowania się opcjami dostępnymi na login.gov.pl. c. Autoryzacja LDAP – dla użytkowników wewnętrznych Zamawiającego. 2. Pozwalający na dostęp użytkowników z różnymi rodzajami urządzeń (laptop, smartfon, tablet) i systemami operacyjnymi (Windows, Android, IOS, Linux, Unix). 3. Główny Serwer Systemu z macierzą dyskową oraz maszynami wirtualnymi (VM) realizującymi poszczególne funkcje systemu.
2.	Sieć i bezpieczeństwo	Sieć - Ethernet, xDSL,3G/4G/5G, WiFi, WiMAX. Bezpieczeństwo sieciowe zgodne z wymaganiami – NGFW.
3.	Standardy wymiany danych	Standardy zgodne z wymaganiami - HTTPS Użycie protokołu TLS 1.3 oraz certyfikatów SSL 2.0, SSL 3.0
4.	Systemy operacyjne serwerowe	Debian Linux
5.	Bazy danych	PostgreSQL
6.	Serwery aplikacji	NGINX
7.	Portale	- Portal Web - Mapping of Broadband Services in Europe, EC - PRO Speed Test (VSPEED Sp. z o.o)
8.	Inne	Webowe interfejsy graficzne użytkowników E-Usługi z funkcjami interaktywnej mapy i formularzy elektronicznych, aktywne *dashboardy*. Wykorzystanie wirtualizacji opartej na Vmware. Wykorzystanie środowiska uruchomieniowego opartego na konteneryzacji (np. Kubernetes)

7.3. Wymagania w zakresie infrastruktury Systemu

Zakup infrastruktury:

Zakup urządzeń pomiarowych mobilnych – zakup 4 000 szt. mobilnych stacji pomiarowych.

Zakup urządzeń pomiarowych - stacje pomiarowe – zakup 17 szt. stacji pomiarowych.

7.4. Wymagania w zakresie metody pomiaru

WMP-1. Możliwość przeprowadzania testów ciągłych, dających informacje na temat parametrów łącza w czasie.

WMP-2. Wyeliminowanie czynników zewnętrznych, takich jak stacja kliencka w procesie pomiarowym.

Monitorowanie bezpieczeństwa sieci będzie odbywało się poprzez pasywne monitorowanie przepływów sieciowych w celu poszukiwania charakterystyk ataków takich jak:

- ataki DoS/DDoS,
- ataki oraz uczestnictwo w botnetach,
- ataki na protokoły trasowania (BGP, vlan spoofing oraz inne),
- anomalia bezpieczeństwa sieci,
- inne ataki na sieć PT oraz UK,
- kompromitacja sieci i urządzeń użytkownika:
    - uczestnictwo sieci oraz urządzeń w klastrach botnet,
    - połączenia z sieci użytkownika do szkodliwych sieci orz urządzeń, takich jak serwery Command-and-Control (C&C),
    - inne parametry bezpieczeństwa sieci oraz urządzeń,
    - uczestnictwo w atakach typu „zombie”,
    - połączenia z niebezpiecznymi sieciami oraz urządzeniami;
- inne ataki sieciowe.

Dzięki zbudowaniu sieci próbników pomiarowych oraz zintegrowania ich z centralnym systemem zbierania oraz raportowania danych możliwe stanie się:

- pomiar oraz porównywanie parametrów łącza (w tym parametrów bezpieczeństwa łącza) pomiędzy:
    - regionami,
    - operatorami IAS,
    - przedziałami czasowymi,
    - rodzajami pomiarów oraz parametrów.
- raportowanie oraz agregowanie danych bezpieczeństwa do centralnej bazy danych

przekazywanie oraz integracja danych, w tym przekazywanie danych o anomaliach do odpowiednich ISAC oraz CSIRT poziomu krajowego.

Dzięki korelacji wyników pomiędzy tymi 2 typami próbników, możliwe stanie się wykrywanie anomalii sieci takich jak:

- nadmierne obciążenie sieci w danym rejonie geograficznym;
- ataki na węzły sieciowe;
- ataki na systemy operatorskie;
- ataki na segmenty sieci w tym:
    - wybrane podsieci;
    - wybranych operatorów;

- wybranych klientów;
- wybrane lokalizacje

Powyższe pomiary łącza sieciowego będą mogły być dokonywane w sposób ciągły oraz niezależny, dzięki wykorzystaniu urządzeń oraz oprogramowania urządzeń stworzonych w ramach projektu. Dzięki ciągłości pomiarów bezpieczeństwa oraz parametrów łącza, możliwe stanie się skuteczniejsze wykrywanie zagrożeń oraz uchybień w zakresie parametrów jakościowych oraz ilościowych łącza. Dzięki wykorzystaniu niezależnych urządzeń (w przeciwieństwie do stosowania np. stacji użytkownika do pomiarów łącza), wyeliminowane zostaną wszelkie problemy związane z czynnikami zewnętrznymi występującymi w pomiarach z użyciem współdzielonych stacji roboczych. Zastosowanie próbników umożliwi także szybsze raportowanie oraz reagowanie na wykryte nieprawidłowości oraz zagrożenia, a także dokonywanie ciągłych pomiarów w czasie w celu zbudowania realnego obrazu parametrów łącza (w przeciwieństwie do parametrów łącza jedynie w danym punkcie czasu).

7.5. Wymagania w zakresie próbników konsumenckich

Zasady pomiaru i metodologia pomiarowa powinna w jak największym stopniu (uzależnionym od przyjętych rozwiązań technicznych) powinna uwzględniać wytyczne BEREC w zakresie metodologii pomiarowych.

Obejmuje to poniższe dokumenty lub ich zaktualizowane wersje (na dzień ogłoszenia zamówienia publicznego):

1. BoR (20) 112, BEREC Guidelines on the Implementation of the Open Internet Regulation, https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/9277-berec-guidelines-on-the-implementation-of-the-open-internet-regulation
2. BoR (17) 178, BEREC Net Neutrality Regulatory Assessment Methodology, https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/methodologies/7295-berec-net-neutrality-regulatory-assessment-methodology
3. BoR (14) 117, Monitoring quality of Internet access services in the context of net neutrality BEREC report, http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/4602-monitoring-quality-of-internet-access-services-in-the-context-of-net-neutrality-berec-report

Mając na uwadze ww. dokumenty, w zakresie konsumenckim system powinien umożliwiać pomiar w szczególności następujących parametrów:

a. Prędkość pobierania i wysyłania danych mierzona jako przepływność TCP w Mb/s, zgodnie z opisaną poniżej metodą.
b. Opóźnienie rozumiane jako np.: ping lub 3-way-handshake TCP (RTT). Wyniki testu powinny zawierać wartości w ms przed wykonaniem testu oraz uśrednione wartości z periodycznych pomiarów w trakcie jego trwania. Różnica pomiędzy dwoma wielkościami opóźnienia powinna być dostępna w raporcie jako parametr Buffer Delay (zgodnie z IETF RFC 6349).
c. Zmienność opóźnienia (jitter) rozumiana jako różnica z periodycznych pomiarów opóźnienia w trakcie generowanego ruchu testowego w ms.
d. Retransmisje TCP jako informacja o ilości utraconych pakietów podczas transmisji w %.

System powinien pozwalać na pomiar prędkości transmisji danych do 2,5 Gb/s w obu kierunkach (sekwencyjnie).

Wynik pomiaru prędkości transmisji danych uzyskany przy pomocy aplikacji powinien być zgodny z wynikiem pomiaru uzyskanym przy zastosowaniu metody opisanej w dokumencie IETF RFC 6349.

Pomiar prędkości transmisji danych, w kierunku pobierania i wysyłania danych, powinien odbywać się według opisanej metody:

a. W celu wykonania pomiaru prędkości pobierania i wysyłania danych, inicjowana jest, przy pomocy protokołu TCP, transmisja danych pomiędzy sondą konsumencką a serwerem testowym.
b. Transmitowane dane nie podlegają kompresji.
c. Warunki transmisji danych w trakcie pomiaru zapewniają wysycenie pojemności łącza.
d. Prędkość pobierania danych mierzona jest dla kierunku transmisji danych od serwera testowego do sondy konsumenckiej.
e. Prędkość wysyłania danych mierzona jest dla kierunku transmisji danych od sondy konsumenckiej do serwera testowego.
f. Wskaźnik prędkości pobierania i wysyłania danych określa się na podstawie ilości danych przesłanych w czasie pomiaru i wyraża w megabitach na sekundę (Mb/s).
g. Do określenia ilości przesłanych danych wykorzystuje się dane przenoszone w segmentach protokołu TCP.
h. Czas pojedynczego pomiaru wynosi co najmniej 15 sekund dla każdego z kierunków transmisji niezależnie i obejmuje fazę wysycenia pojemności łącza.

Lista dodatkowych czynników związanych z warunkami wykonania pomiaru, których możliwie jak najwięcej z nich (z uwzględnieniem przyjętych rozwiązań technicznych) powinien uwzględniać i identyfikować system pomiarowy:

a. Data i godzina pomiaru z dokładnością do 1 sekundy.
b. Prywatny oraz publiczny adres IP przydzielony przez operatora sieci.
c. Nazwa operatora sieci (np. na podstawie publicznego adresu IP).
d. Interfejsy sieciowe komputera użytkownika ze wskazaniem połączenia wykorzystanego do testu (WiFi, Ethernet, VPN itp.).
e. Typ/model karty sieciowej oraz prędkość i dupleks połączenia sieciowego komputera użytkownika.
f. Parametry radiowe w przypadku wykorzystania interfejsu radiowego, w szczególności rodzaj połączenia: 802.11b/g/n/a/ac, RSSI, SNR oraz szybkość transmisji: 11Mb/s, 54Mb/s itd.
g. Obciążenie interfejsu sieciowego, procesora i pamięci operacyjnej komputera użytkownika przed i w trakcie pomiaru.
h. Podstawowe dane o konfiguracji komputera klienta (np. CPU, RAM).
i. Rodzaj i wersja systemu operacyjnego zainstalowanego na komputerze użytkownika.
j. Wielkość ruchu w tle (cross-traffic) z/do komputera użytkownika, na którym uruchomiono aplikację pomiarową, równoczesnego z ruchem związanym z wykonaniem pomiaru.
k. Droga sieciowa (traceroute) pomiędzy komputerem użytkownika i serwerem testowym (co najmniej adresy IP).
l. Lista aktywnych procesów w trakcie trwania testu.

m. Tablica ARP komputera, z którego realizowany był pomiar. Tablica ARP powinna być wyczyszczona przed pomiarem i ustalona na podstawie skanowania podsieci IP.

n. Liczba równoległych sesji oraz wielkość okna transmisyjnego TCP (window size wg IETF RFC 1323) wykorzystanego podczas pomiaru.

o. Buffer Delay (zgodnie z IETF RFC 6349).

p. Aktywne połączenia VPN.

q. Udostępnianie Internetu na urządzeniu końcowym użytkownika.

r. Aktywny firewall.

s. Oznaczenie wykorzystanego serwera testowego.

t. Sposób zasilania przenośnego urządzenia końcowego użytkownika.

System pomiarowy powinien umożliwiać użytkownikowi realizację pomiarów certyfikowanych w rozumieniu art. 4 ust. 4 Rozporządzenia o Otwartym Internecie (2015/2120). W tym celu pomiar powinien być zrealizowany w takich warunkach, które zagwarantują jego wynikowi określoną moc dowodową i nie będą w sposób oczywisty, łatwy i niewymagający kosztów falsyfikowane.

Użytkownik powinien posiadać możliwość realizacji pomiarów sekwencyjnych i cyklu pomiarów.

WPK-1. Niewielkie urządzenia pomiarowe pozwalające na zamontowanie oraz analizę w przyłączu Użytkownika Końcowego.

WPK-2. Zasilanie urządzenia z wykorzystaniem standardu USB Power Delivery[15] lub Power Over Ethernet[16].

WPK-3. Monitorowanie jakości sieci dostawcy usługi IAS.

WPK-4. Monitorowanie bezpieczeństwa sieci dostawcy usługi IAS.

WPK-5. Monitorowanie bezpieczeństwa sieci Użytkowników Końcowych.

WPK-6. Wraz z próbnikami stworzone zostanie dedykowane oprogramowanie wspierające, zawierające w sobie logikę oraz algorytmy pomiarów parametrów oraz bezpieczeństwa łącza internetowego a także oprogramowanie frontend oraz backend próbników, pozwalające na interakcję użytkownika z próbnikiem za pomocą dedykowanego panelu web, dostępnego po podłączeniu próbnika do sieci lokalnej.

WPK-7. Zamawiający przewiduje certyfikację próbników przez niezależną organizację zewnętrzną.

7.6. Wymagania w zakresie próbników sieciowych

WPS-1. Próbnik sieciowy do urządzenia pomiarowe montowane na węzłach sieci PT, pozwalające na analizę łącza bezpośrednio w sieci operatorskiej. Charakteryzowały się one będą większą przepustowością oraz większymi możliwościami analizy, dzięki braku ograniczeń takich jak wielkość urządzenia.

WPS-2. Monitorowanie jakości sieci dostawcy usługi IAS.

WPS-3. Monitorowanie bezpieczeństwa sieci dostawcy usługi IAS.

WPS-4. Wraz z próbnikami stworzone zostanie dedykowane oprogramowanie wspierające, zawierające w sobie logikę oraz algorytmy pomiarów parametrów oraz bezpieczeństwa łącza internetowego a także oprogramowanie frontend oraz backend próbników, pozwalające na

[15] USB Power Delivery, Base Specification, https://www.usb.org/document-library/usb-power-delivery
[16] PoE zgodny ze standardami z grupy IEEE 802.3

interakcję użytkownika z próbnikiem za pomocą dedykowanego panelu web, dostępnego po podłączeniu próbnika do sieci lokalnej.

WPS-5. Czas potrzebny na instalację i uruchomienie pojedynczego próbnika sieciowego nie może przekraczać 60 minut.

7.7. Wymagania w zakresie raportów

WRa-1. System umożliwia sporządzanie raportów okresowych wg podanego przedziału czasu, określonego za pomocą dat i czasu z dokładnością do minut w zakresie:

a. Liczby przeprowadzonych testów jakości usług IAS z możliwością podziału na:
   i. metodę lub sposób wynikający z metody wykonania testu,
   ii. klasyfikację pomiaru: certyfikowany i nie certyfikowany,
   iii. obszar podziału administracyjnego Polski z dokładnością do miejscowości.

b. Wartości mierzonych podczas testów jakości usług IAS z możliwością podziału na:
   i. wielkości podlegające pomiarowi,
   ii. obszar podziału administracyjnego Polski z dokładnością do miejscowości.

c. Liczby zgłoszeń przyjętych za pomocą E-Usługi z możliwością podziału na:
   i. obszar podziału administracyjnego Polski z dokładnością do miejscowości.

d. Liczby obsłużonych reklamacji z możliwością podziału na:
   i. obszar podziału administracyjnego Polski z dokładnością do miejscowości.

e. Liczby wyświetleń E-Usługi z możliwością podziału na:
   i. obszar podziału administracyjnego Polski z dokładnością do miejscowości.

f. Liczby i rodzaju wprowadzonych do rejestru publicznego, o którym mowa w rozdziale 6.2, danych.

WRa-2. Raporty sporządzane z użyciem Systemu pozwalają na grupowanie danych wg:

a. czasu: godziny, doby, tygodnia, miesiąca, roku,

b. obszaru podziału administracyjnego Polski: miejscowości, gminy, powiatu, województwa,

i wyznaczanie dla grup danych oraz całego zakresu raportu: sum, wartości średnich i median dla wartości wielkości liczbowych ujętych w raporcie.

7.8. Wymagania w zakresie interfejsów graficznych użytkowników

WIG-1. System musi posiadać interfejs użytkownika w języku polskim, praca oraz raportowanie musi być możliwe w języku polskim, forma graficzna interfejsu musi uwzględniać kolorystykę właściwej dla stron internetowych Zamawiającego (UKE).

WIG-2. System musi umożliwiać dostosowywanie interfejsu w zakresie kroju czcionek, ich wielkości oraz kolorystki wszystkich elementów interfejsu.

WIG-3. System musi sygnalizować stan wykonywania zadanej operacji (np. za pomocą ikony klepsydry, czasomierza itp.).

WIG-4. System musi umożliwiać modyfikację szerokości kolumn w prezentowanych widokach tabelarycznych.

WIG-5. Graficzna prezentacja wyników pomiarów będzie przedstawiona w taki sposób, aby nie utracić czytelności obrazu mając na względzie rozdzielczość ekranu.

WIG-6. System podczas wykonywania zadania pomiarowego musi wyświetlać na ekranie parametry i wyniki adekwatne do wykonywanego zadania.

WIG-7. System musi umożliwiać wyszukiwanie raportów archiwalnych zawartych w bazie.

WIG-8. System musi umożliwiać definiowanie kryteriów wyszukiwania co najmniej:

1. Z użyciem dowolnego zestawu danych zawartych bazie danych łączonych za pomocą operatorów logicznych,
2. Z użyciem wyszukiwania pełnotekstowego,
3. Z użyciem znaków: znaku „*” określającego dowolny ciąg znaków i znaku „?” określającego dowolny pojedynczy znak.

WIG-9. System musi umożliwiać wspomaganie wyszukiwania danych poprzez użycie kreatora wyszukiwania oraz poprzez bezpośrednie wpisywanie zapytań.

WIG-10. System musi zapewnić możliwość filtrowania i sortowania danych otrzymanych w wyniku wyszukiwania.

WIG-11. System musi zapewnić możliwość zapisywania danych otrzymanych w wyniku wyszukiwania co najmniej w formatach: pdf oraz strukturalnym tekstowym, np. csv.

WIG-12. System musi zapewnić:

1. wyświetlanie wygenerowanego raportu na ekranie stacji roboczej,
2. zapisanie raportu co najmniej w formatach: pdf, docx
3. wydruk raportu.

WIG-13. Wykonawca stworzy gotowe, predefiniowane szablony raportów.

WIG-14. System musi zapewnić tworzenie raportów w oparciu o dane znajdujące się w bazach.

WIG-15. System musi posiadać funkcję pomocy, która będzie elementem Systemu.

WIG-16. System musi zapewnić wbudowaną pomoc kontekstową z możliwością jej wyłączenia.

WIG-17. System w przypadku braku możliwości wykonania pomiaru musi wyświetlać powiadomienie o niedostępności elementu infrastruktury pomiarowej z wykorzystaniem interfejsu.

WIG-18. Wykonawca zaproponuje rozwiązanie szczegółowe dotyczące obsługi archiwizacji danych i dostępu do nich.

WIG-19. System musi być zgodny z wytycznymi WCAG 2.1 na poziomie AA.

7.9. Zasoby dla Systemu

Dla zapewnienia ciągłości działania budowanego systemu usługi będą świadczone w dwóch centrach operacyjnych połączonych ze sobą odpowiedniej jakości i przepustowości łączem. Zamawiający rozważa dwa scenariusze realizacji tego wymagania:

- Wykorzystanie podstawowego ośrodka przetwarzania danych UKE w Boruczy (przechowywanie, przetwarzanie) oraz zapasowego w Warszawie.

  W takim przypadku Wykonawca w ramach zamówienia dostarczy niezbędne zasoby do budowy Systemu w szczególności serwery, przestrzeń dyskową i inne kompatybilne z infrastrukturą Zamawiającego wraz z niezbędnymi licencjami na wykorzystane oprogramowanie (wirtualizacja, kopie zapasowe, zarządzanie).

- Wykorzystanie usług chmurowych.

Tabela 5 - Minimalne wymagania sprzętowe na potrzeby środowiska produkcyjnego i testowego

Lp.	Komponent	Jednostka miary	Wartość minimalna
1	Moc obliczeniowa serwerowni	teraflopsy	10
2	Baza danych	rekord w bazie danych	1 00 000
3	Konteneryzacja & serwery	Rdzeń CPU	240
4	Konteneryzacja & serwery	RAM w GB	512
5	Konteneryzacja & serwery	Przestrzeń dyskowa w GB	1 000
6	Serwer plików frontend	Przestrzeń dyskowa w GB	100
7	Serwer plików backend	Przestrzeń dyskowa w GB	20 000

Moc obliczeniowa serwerowni zostanie potwierdzona za pomocą testu LINPACK Benchmark.

7.10. Wymagania w zakresie bezpieczeństwa

WB-1. Wykonawca zobowiązany jest do opracowania architektury bezpieczeństwa E-Usługi oraz SMJI.

WB-2. W ramach Projektu System będzie poddawany testom bezpieczeństwa przed wdrożeniem jak i podczas użytkowania - co najmniej jeden raz w roku. Wykonawca zobowiązany będzie do udziału i współpracy z zespołem testowym w czasie przeprowadzania testów oraz będzie zobowiązany do wdrożenia rekomendacji opracowanych przez zespół testowy. Testy te zostaną zlecone podmiotowi zewnętrznemu specjalizującemu się w wykonywaniu testów bezpieczeństwa.

WB-3. Wykonawca zobowiązany jest do zastosowania podejścia „Security by Design" poprzez dobranie i implementację właściwych mechanizmów bezpieczeństwa, adresujących wymagania funkcjonalne i niefunkcjonalne oraz minimalizujących skutki lub eliminujących możliwość materializacji znanych zagrożeń, co najmniej w zakresie przytoczonych niżej zasad bezpieczeństwa OWASP[17]:

1. **Minimalizowanie powierzchni ataku** *(ang. Minimize attack surface area)* – każda funkcjonalność dotycząca wymiany informacji z otoczeniem (interfejs użytkownika, interfejs komunikacji z zewnętrznym systemem, ładowanie plików) niesie za sobą ryzyko wystąpienia błędu skutkującego możliwością zaistnienia podatności systemu. W celu zapewnienia bezpieczeństwa istotnym jest ograniczanie tego ryzyka już na etapie wytwarzania.
2. **Stosowanie domyślnego poziomu bezpieczeństwa** (*ang. Establish secure defaults*) – zastosowane mechanizmy bezpieczeństwa powinny mieć domyślnie ustaloną politykę działania na włączoną, np. weryfikacja złożoności hasła użytkownika, wymuszanie zmiany hasła po określonej liczbie dni, itp.
3. **Nadawanie minimalnych uprawnień** (*ang. Principle of Least privilege*) – każde z kont użytkownika lub usługi powinno posiadać minimalny zestaw uprawnień do zasobów, niezbędny do realizowania założonej funkcjonalności, np. usługa powinna być

[17] Security by Design | ESDC Security Knowledge Portal, https://esdcskp-edscpcs.github.io/skp/security-by-design/

uruchamiana z uprawnieniami dedykowanego dla niej konta nie posiadającego uprawnień nadmiarowych.

4. **Ochrona w głąb** *(ang. Principle of Defense in depth)* – w Systemie zastosowane są mechanizmy bezpieczeństwa na kilku warstwach, w celu utrudnienia ich przełamania.
5. **Kontrolowane działanie w przypadku wystąpienia błędu** (*ang. Fail securely*) – w przypadku wystąpienia błędu lub wyjątku System powinien w sposób kontrolowany przejmować ich obsługę, informując o wystąpieniu błędu lub - w sytuacjach krytycznych – kończąc swoje działanie po zapisaniu do dziennika informacji o zaistniałym zdarzeniu.
6. **Brak zaufania do zewnętrznych usług** *(ang. Don't trust services)* – w wielu przypadkach elementem systemu są usługi dostarczane przez zewnętrzne podmioty, których zasady i polityki bezpieczeństwa są poza kontrolą Zamawiającego. W związku z tym, Zamawiający oczekuje aby we wszystkich przypadkach polegania na zewnętrznych usługach wprowadzone zostały mechanizmy zapewniające autentyczność usługi oraz weryfikujące poufność, integralność danych dostarczanych przez usługę oraz dostępność usługi.
7. **Rozdział obowiązków** (*ang. Separation of duties*) – w ramach E-Usługi oraz SMJI występują różne role, które powinny mieć swoje odzwierciedlenie w systemie uprawnień. Stąd Wykonawca winien dokonać starannego doboru uprawnień do zdefiniowanych ról.
8. **Unikanie budowania bezpieczeństwa przez niejawność** (*ang. Avoid security by obscurity*) – bezpieczeństwo Systemu i E-Usługi nie może opierać się na utajnieniu całego rozwiązania lub części: technologii, architektury, kodu źródłowego, użytych komponentów czy też zastosowanych algorytmów kryptograficznych. Powinno ono opierać się na ściśle określonych elementach, dla których można monitorować podatności i określić cząstkowe wskaźniki podatności, np. wartości metryk w metodzie CVSS[18].
9. **Zaprojektowanie mechanizmów w sposób prosty i przejrzysty** *(ang. Keep security simple)* – zastosowanie tej zasady ma na celu obniżenie ryzyka wystąpienia błędu skutkującego podatnością poprzez eliminację zbędnych złożoności w zakresie architektury i algorytmów w ramach E-Usługi oraz SMJI.
10. **Prawidłowe usuwanie błędów związanych z bezpieczeństwem** *(ang. Fix security issues correctly)* – w przypadku usuwania błędów związanych z mechanizmami bezpieczeństwa czy też z bezpieczeństwem całego Systemu lub E-Usługi istotnym jest przeprowadzenie dochodzenia w celu zidentyfikowania przyczyny wystąpienia błędu i stosownych testów w celu potwierdzenia prawidłowego zidentyfikowania przyczyny wystąpienia błędu.

WB-4. Dla każdej warstwy architektury Systemu i E-Usługi powinny być zastosowane i udokumentowane odpowiednie mechanizmy bezpieczeństwa: fizyczne, proceduralne, techniczne i prawne, odpowiadające zasadom określonym w punkcie WB-3.

WB-5. Bezpieczeństwo warstwy transportowej przy zestawianiu połączeń między Systemem i systemami utrzymywanymi przez kwalifikowanych dostawców usług wymaga uwierzytelnienia zarówno po stronie klienta jak i serwera za pomocą certyfikatów (tzw. „mutual authentication").

[18] Common Vulnerability Scoring System, Forum of Incident Response and Security Teams, https://www.first.org/cvss/specification-document

WB-6. Autoryzacja żądań od systemów zintegrowanych z SMJI wymaga użycia protokołu OAuth2 (możliwość wykorzystania walidacji tokenów HMAC oraz kodów autoryzacyjnych przekazywanych do klienta) przy udziale połączenia szyfrowanego.

WB-7. Identyfikacja i uwierzytelnianie użytkowników wewnętrznych, uprawnionych przez Zamawiającego wykorzysta CSU Zamawiającego.

WB-8. Identyfikacja i uwierzytelnianie użytkowników zewnętrznych (nie posiadających konta w CSU Zamawiającego) wykorzysta Profil Zaufany lub odpowiedni system lub usługę dostępną przez krajowego brokera usług w przyszłości.

WB-9. Uwierzytelnienie użytkowników w graficznym interfejsie wymaga środka identyfikacji elektronicznej na poziomie zaufania średnim lub wysokim.

WB-10. Autoryzacja użytkowników wykorzystuje przyznane w SMJI uprawnienia. Zakres danych i dostęp do określonych funkcjonalności będzie ograniczony do przypisanych ról.

WB-11. Administratorzy systemu wykorzystują dostęp do szerszego zakresu danych (np. logi) i funkcjonalności (np. konfiguracje), zgodnie z zapotrzebowaniem wynikającym z pełnionej roli w ramach wskazanego komponentu.

WB-12. W celu zapewnienia bezpieczeństwa komunikacji muszą być spełnione następujące warunki:

1. Komunikacja w sieci publicznej odbywa się za pomocą połączenia szyfrowanego (np. VPN, TLS).
2. Implementowane algorytmy oraz wersje TLS używane do szyfrowania połączenia będą:
   a. Odporne na ataki implementacyjne (np. BEAST, CRIME, SWEET32, itd.);
   b. Zapewniały poufność komunikacji historycznej nawet w przypadku wycieku klucza prywatnego używanego do szyfrowania połączenia (ang. *Perfect Forward Secrecy*);
   c. Odporne na ataki typu „*downgrade*", które obniżają bezpieczeństwo połączenia;
   d. Zgodne z rekomendacjami oraz standardami rynkowymi.

Wobec powyższych wymagań celowe jest zastosowanie protokołu TLS w wersji 1.3.

Wymiana informacji pomiędzy e-usługami wchodzącymi w skład Projektu zostanie dodatkowo zabezpieczona mechanizmami takimi jak certyfikaty klucza publicznego czy unikalne klucze dostępowe.

WB-13. Przychodzące wiadomości będą odbierane, a następnie składowane w bazie danych lub dedykowanych mechanizmach składowania danych. Wszystkie załączniki powinny być zapisane na dedykowanym zasobie dyskowym, a metadane załączników wraz z lokalizacją powinny trafić do bazy danych. W celu ochrony integralności danych w metadanych powinien znaleźć się wyliczony z zawartości pliku skrót kryptograficzny (ang. *hash*). Wyliczany skrót powinien być wykonany za pomocą algorytmu SHA-2. Pliki składowane będą w postaci zaszyfrowanej, z wykorzystaniem szyfrowania symetrycznego lub asymetrycznego. Zaszyfrowane dokumenty w momencie przetwarzania będą odszyfrowywane „w locie", następnie zostaną one ponownie zaszyfrowane w momencie ponownego ich zapisu.

WB-14. Zgodne z §20 KRI, E-Usługa realizowana za pomocą SMJI, stanowi typowy podsystem zarządzania bezpieczeństwem (w tym bezpieczeństwa i ochrony danych) informacji i ma spełniać wymagania Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:

1. PN-ISO/IEC 27002 w odniesieniu do ustanawiania zabezpieczeń (jako minimalne wymagania dla rejestrów publicznych i wymiany informacji w postaci elektronicznej);
2. PN-ISO/IEC 27005 w odniesieniu do zarządzania ryzykiem.

Wymagania dodatkowe - dla tego typu projektów bazodanowych „big-data" z interfejsem klienckim z zastosowaniem modelu klient- serwer – wymagają zapewnienia właściwego doboru i konfiguracji komponentów sprzętowych i programowych projektu (e-usługi) pod kątem bezpieczeństwa, i stąd mają obejmować:

a. w przypadku baz danych: bieżącą aktualizację oprogramowania bazy danych, analizę zastosowanych metod uwierzytelniania, sprawdzenie polityki haseł, sprawdzenie mechanizmów przechowywania haseł, logowania zdarzeń, archiwizacji danych, analizę i ocenę mechanizmów kontroli dostępu fizycznego i logicznego,
b. w przypadku komponentów sprzętowych: bieżącą aktualizację oprogramowania komponentu, zapewnienia mechanizmu analizy i oceny sposobu obsługi błędów, analiz metod.
c. struktura Systemu będzie poprzez rozwiązania architektoniczne spełniała wysokie standardy m.in. zapewnienie ciągłości działania, jako dostawca szeregu usług oferowanych w reżimie 24/7, oraz standardy bezpieczeństwa i ochrony informacji.

WB-15. Wykonawca zobowiązany jest do rozpatrzenia podstawowych aspektów bezpieczeństwa aplikacji, które mają wpływ na bezpieczeństwo całości Systemu, takich jak:

1. **Zabezpieczenie aplikacji przed przeciążeniem** – wymiarowanie środowiska produkcyjnego zostanie przeprowadzone na podstawie szacowań obciążenia. Wykonawca zobowiązany jest zastosować mechanizmy do równoważenia obciążenia (*load balancing*) w klastrach, które będą rozmieszczone w rożnych centrach obliczeniowych. W celu eliminacji hipotetycznego obciążenia pochodzącego z ataków typu DDoS lub innej niepożądanej komunikacji, zastosować odpowiednie zabezpieczenia typu IPS/IDS. Architektura oraz komponenty Systemu powinny zostać tak dobrane, aby zapewnić łatwe i szybkie skalowanie poziome. Jednocześnie - zgodnie z wytycznymi dotyczącymi jakości kodu – Zamawiający oczekuje wyeliminowania nieefektywnych wydajnościowo elementów w procesie analizy kodu.
2. **Zabezpieczenie aplikacji przed awarią** – w tym zakresie Wykonawca zobowiązany jest do stosowania zasady wskazanej w punkcie WB-3.5 (*Fail securely*) oraz do zapewnienia wysokiej dostępności aplikacji rozproszonych przy spełnieniu warunków szczególnych:
   a. Serwery aplikacyjne będą zagregowane w jednostki logiczne typu klaster, które będą zreplikowane w dwóch lokalizacjach (takich jak *Availability Zones* czy centra danych).
   b. Serwery bazy danych stworzą jednostkę typu *High Availability* (HA) zapewniającą odporność na awarie.
   c. Zostanie wprowadzony system kolejkowania wiadomości, który zapewni wysoką przepustowość, bezpieczeństwo, skalowalność i replikację komunikatów w poszczególnych węzłach.
   d. Zostanie wykorzystany rozproszony system plików (ang. *Distributed File System*), który zmniejszy ryzyko utraty i zwiększy dostępność danych przy awarii jednego serwera oraz umożliwi rozłożenie obciążenia na wiele rożnych maszyn.

e. Zgodnie z wymaganiami dotyczącymi jakości kodu zostanie wykonana automatyczna analiza przepływu danych celem eliminacji a co najmniej ograniczenia prawdopodobieństwa wystąpienia wycieków pamięci w aplikacji.

3. **Zabezpieczenie przed nieuprawnionym dostępem** – Wykonawca zaimplementuje zabezpieczenia wielopoziomowe w celu wprowadzenia zabezpieczeń przed nieuprawnionym dostępem, w szczególności:

a. w obszarze uwierzytelnienia (za pomocą środka identyfikacji elektronicznej na poziomie zaufania średnim lub wysokim) i autoryzacji;

b. wykorzystanie narzędzi do wykrywania intruzów: IDS;

c. ograniczenie podatności przejęcia kontroli nad stroną webową poprzez zastosowanie dedykowanych blokad aplikacyjnych (Web Application Firewall - WAF);

d. wprowadzenie zapory sieciowej firewall;

e. wdrożenie kontroli uprawnień dla aplikacji i Systemu.

4. **Zdefiniowanie i kontrola uprawnień** – Wykonawca zobowiązany jest do zdefiniowania uprawnień użytkowników i administratorów zgodnych (koniecznych i wystarczających) z rolami biznesowymi na rożnych płaszczyznach, zgodnie z zasadą rozdziału uprawnień oraz najmniejszych uprawnień użytkownika.

5. **Monitorowanie działania aplikacji** – monitorowanie poprawności oraz stabilności działania powinno odbywać się na kilku płaszczyznach:

c. monitorowanie infrastruktury (I/O, CPU, RAM, dostępne miejsce w systemie plików);

d. monitorowanie aktywności użytkowników;

e. monitorowanie ruchu sieciowego.

6. **Wyselekcjonowane możliwe zagrożenia** będą generowały alerty lub powiadomienia odpowiednio do poziomu zagrożenia w celu podjęcia odpowiednich działań przez administratorów lub osoby posiadające odpowiednie uprawnienia. Wykonawca zobowiązany jest do stworzenia lub wykorzystania istniejącego systemu do agregacji i prezentacji wybranych logów.

7. **Zapewnienie ciągłości działania** – Zamawiający wymaga aby System był obsługiwany przez dwa centra operacyjne pracujące równolegle z odpowiedniej jakości i przepustowości łączem dla potrzeb komunikacji. Wykonawca zapewni możliwość tworzenia kopii bezpieczeństwa danych i ich przechowywania w bezpieczny sposób. Kopie bezpieczeństwa muszą być wykonane w taki sposób, aby zawsze była możliwość odtworzenia Systemu (*Bare-Metal Recovery*) jak również odtwarzania poszczególnych jego elementów i zakresów danych. W ramach niniejszego zamówienia, Zamawiający wymaga odpowiedniego rozszerzenia pamięci masowej dla systemu przechowywania kopii zapasowych opartego na macierzy NetApp oraz rozszerzenia posiadanych licencji oprogramowania do zarządzania kopiami zapasowymi CommVault.

8. **Bezpieczeństwo serwera aplikacji** – Zamawiający wymaga zabezpieczenia serwera aplikacyjnego poprzez:

a. wprowadzenie konfiguracji warstwy transportowej TLS;

b. wprowadzenie zabezpieczeń zgodnych z zaleceniami Open Web Application Security Project (OWASP) ASVS;

c. zastosowanie dodatkowej konfiguracji w zakresie zabezpieczenia (*hardeningu*) oraz ocena konfiguracji w zakresie bezpieczeństwa na podstawie zaleceń i list weryfikacyjnych, np. NIST NCP[19] lub CIS Benchmarks[20] lub analogicznych, opracowanych przez dostawcę systemu operacyjnego[21] czy rozwiązania aplikacyjnego;

d. zostanie zablokowana możliwość pobrania informacji o typie serwera i wersji, zostaną zablokowane zadania pobrania listy katalogów, zostaną zablokowane zadania typu HTTP TRACE i HTTP OPTIONS;

e. wprowadzenie kontroli dostępu zgodnej z wymaganiami bezpieczeństwa;

f. integracje z serwerem HSM (ang. Hardware Security Module).

9. **Testy bezpieczeństwa** – w ramach realizacji zamówienia Zamawiający przewiduje wykonanie testów bezpieczeństwa, odpowiednio:

a. testy penetracyjne i skany bezpieczeństwa, które zostaną wykonane przez podmiot wskazany przez Zamawiającego, zgodnie z założeniami opisanymi w rozdziale 7.10.3;

b. testy jakości oprogramowania, wykonane przez Wykonawcę w ramach realizacji wymagań zawartych w rozdziale **Błąd! Nie można odnaleźć źródła odwołania.**;

c. testy wynikające z analizy bezpieczeństwa kodu, wykonane przez Wykonawcę w ramach realizacji wymagań zawartych w rozdziale 7.10.2.

WB-16. Wykonawca jest zobowiązany do usunięcia wykrytych w ramach testów penetracyjnych błędów i podatności.

WB-17. Zamawiający wymaga aby struktura Systemu poprzez zastosowane rozwiązania architektoniczne spełniała wysokie standardy m.in. w zakresie zapewnienia ciągłości działania, jako dostawca szeregu usług oferowanych w reżimie 24/7, oraz standardy bezpieczeństwa i ochrony informacji. W tym celu Zamawiający wymaga wykorzystania dobrych praktyk zdefiniowanych w następujących normach bezpieczeństwa ISO:

1. PN-ISO/IEC 22301 lub równoważnej - w zakresie systemu zarządzania ciągłością działania w zakresie świadczenia usług związanych z sieciami teleinformatycznymi i cyberbezpieczeństwem.
2. ISO/IEC 24762 - w zakresie systemu i procesu odtwarzania zasobów IT po katastrofie w ramach odtwarzania komponentów niezbędnych do zapewnienia ciągłości działania.
3. ISO 27001 - w zakresie systemu zarządzania bezpieczeństwem informacji w zakresie świadczenia usług związanych z sieciami teleinformatycznymi i cyberbezpieczeństwem.

WB-18. System powinien wykorzystywać komunikację na linii klient-serwer z zastosowaniem protokołu komunikacyjnego HTTP z implementacją szyfrowania komunikacji w postaci protokołu TLS. Wymiana informacji pomiędzy e-usługami wchodzącymi w skład projektu SMJI powinna być dodatkowo zabezpieczona mechanizmami takimi jak certyfikaty klucza publicznego czy unikalne klucze dostępowe.

[19] National Institute of Standards and Technology, National Checklist Program, Checklist Repository, https://ncp.nist.gov/repository

[20] Center for Internet Security, CIS Benchmarks, https://www.cisecurity.org/cis-benchmarks/

[21] Przykład: Securing Debian Manual, https://www.debian.org/doc/manuals/securing-debian-manual/index.en.html

WB-19. API budowanych serwisów zostanie udokumentowana w sposób umożliwiający łatwą integrację. Dokumentacja ta zostanie wykonana za pomocą szeroko przyjętych oraz wspieranych standardów takich jak OpenAPI czy Swagger.

WB-20. System powinien zbierać dane do analizy logi z urządzeń z wykorzystaniem protokołów wymiany informacji o logach systemowych, takich jak: SYSLOG, SNMP, CLF oraz CEF format, LEEF format.

WB-21. System powinien posiadać możliwość zapisywania i przekazywania informacji o wykrytych incydentach bezpieczeństwa do innych systemów za pomocą ustandaryzowanych formatów danych takich jak: XML, JSON, ATOM, CVS, STIX.

WB-22. System powinien posiadać funkcjonalność bieżącej aktualizacji komponentów oprogramowania, pod katem podatności, aktualności wersji, polityki uwierzytelniania tworzenia i zmiany haseł, kontroli i hierarchii dostępu, bezpieczeństwa i archiwizacji przechowywania danych.

WB-23. System powinien posiadać funkcjonalność kontroli efektywności i kompleksowości mechanizmów redundancji, dostępu do oprogramowania systemowego, aktualizacje oprogramowania systemowego pod kątem usuwania luk i aktualizacji jego wersji, zapewnienia pełnej kontroli nad dostępem do fizycznych komponentów architektury.

WB-24. Zapewnienia dostępu do informacji o bezpieczeństwie sieci operatorów oraz konsumentów końcowych, w tym możliwości raportowania w czasie rzeczywistym o zagrożeniach oraz atakach skierowanych w operatorów PT oraz klientów końcowych.

WB-25. Przedsiębiorcy telekomunikacyjni, w tym będący jednocześnie operatorami usług kluczowych, powinni otrzymywać informacje o bezpieczeństwie sieci, w tym alerty czasu rzeczywistego dotyczące występujących ataków oraz zagrożeń bezpieczeństwa w sieci. Dodatkowo w przypadku wykrycia luk bezpieczeństwa lub ataków na sieć, informacje zagregowane w ramach systemu SMJI będą mogły być przekazane do odpowiednich CSIRT poziomu krajowego w celu reakcji oraz obsłużenia ryzyka.

WB-26. Zapewnienia dostępu do niezaprzeczalnych informacji o faktycznej jakości świadczonych usług IAS o odpowiedniej mocy dowodowej w przypadku postępowania reklamacyjnego, przed Prezesem UKE lub sądem.

WB-27. Posiada możliwość filtrowania połączeń wchodzących i wychodzących oraz możliwość odmawiania żądań dostępu uznanych za niebezpieczne, prowadzenie inspekcja stanów, inspekcji, sprawdzając ładunek pakietów i dopasowując sygnatury pod kątem szkodliwych działań, takich jak ataki z wykorzystaniem exploitów i złośliwe oprogramowanie, obsługa wirtualnych sieci prywatnych, oraz monitorowanie ruchu sieciowego i zapisywanie najważniejszych zdarzeń do dziennika (logu).

WB-28. Autoryzacja, uwierzytelnianie i rozliczanie połączeń sieciowych, z możliwością zarządzania elementami infrastruktury systemu z wykorzystanie certyfikatów, w tym ich: wystawiania, weryfikacji i odwoływania.

WB-29. Uniemożliwienie dostępu do sieci próbnikom, które nie posiadają aktualnego oprogramowania, łatek lub zmodyfikowaną konfigurację oprogramowania wskazującą na ryzyko ataku.

WB-30. Umożliwienie administratorom sieci definiowania zasad, takich jak typy próbników lub role użytkowników, którym wolno uzyskać dostęp do obszarów sieci

WB-31. Monitorowanie ruchu sieciowego i na tej podstawie wykrywanie włamań z wykorzystaniem metody polegającej na defragmentacji, łączeniu pakietów w strumienie danych, analizie nagłówków pakietów oraz analizie protokołów aplikacyjnych oraz metody wyszukiwania w pakietach ciągów danych charakterystycznych dla znanych ataków sieciowych.

WB-32. Zarządzanie logami z wielu źródeł, w tym sieci, zabezpieczeń, serwerów, baz danych i aplikacji, zapewniając możliwość konsolidacji monitorowanych danych w celu uniknięcia przeoczenia istotnych zdarzeń. Dzięki przechowywaniu danych historycznych wykonywanie różnorodnych technik korelacji w celu zintegrowania danych z różnych źródeł w użyteczne informacje o zdarzeniach w systemie. Automatyczna analiza skorelowanych zdarzeń w celu poszukiwania incydentów bezpieczeństwa i ich raportowanie w z wykorzystaniem interfejsu użytkownika i interfejsów do innych systemów.

7.10.1. Bezpieczeństwo danych osobowych

BDO-1. Tworzone systemy będą uwzględniały wymagania zawarte w RODO, Zasoby uczestniczące w przetwarzaniu danych osobowych będą monitorowane oraz zostanie zaplanowany i przeprowadzony audyt bezpieczeństwa (w oparciu o polską normę PN-ISO/IEC 27001).

BDO-2. Obowiązkiem Wykonawcy jest zapewnienie i udokumentowanie przestrzegania podstawowych zasad przetwarzania danych osobowych zgodnie z treścią RODO, w szczególności:

1. **Zasada zgodności z prawem, rzetelności przejrzystości** – dane osobowe muszą być przetwarzane zgodnie z prawem, tj. musi istnieć podstawa prawna przetwarzania tych danych, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą, tzn. informacje dotyczące zbierania, wykorzystywania lub wszelkich innych sposobów przetwarzania danych oraz zakresu, w jakim te dane są lub będą przetwarzane przez administratora SMJI muszą być znane i zrozumiałe dla tych osób.
2. **Zasada ograniczonego celu** – dane muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.
3. **Zasada minimalizacji danych** – dane mogą być przetwarzane w zakresie adekwatnym, stosownym i ograniczonym do celu, w którym zostały zebrane.
4. **Zasada prawidłowości** – dane muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe były prawidłowe i w razie potrzeby uaktualniane, a dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.
5. **Zasada ograniczonego przechowywania** – dane muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez czas ograniczony do ścisłego minimum, nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane (retencja danych).
6. **Zasada integralności i poufności** – przetwarzanie danych musi odbywać się w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, poprzez stosowanie odpowiednich środków technicznych lub organizacyjnych.

7. **Zasada rozliczalności** – administrator danych musi być w stanie wykazać przestrzeganie wszystkich powyższych zasad (prowadzenie odpowiedniej dokumentacji oraz zapewnienie dowodów stosowania powyższych zasad).

BDO-3. Przestrzeganie zasad przytoczonych w punkcie BDO-2 zobowiązuje w szczególności Wykonawcę do zastosowania odpowiednich środków technicznych i organizacyjnych związanych ze spełnieniem wymagań poprzez:

1. Regularne kontrolowanie jakości działania systemów zgodnie z określonym harmonogramem, sposobem i procedurą.
2. Audyt stosowanych algorytmów.
3. Stosowanie zasady minimalizacji danych w procesie zbierania danych oraz odpowiedniej konstrukcji usług formularzowych.
4. Korzystanie z anonimizacji lub pseudonimizacji danych, dla których ustał cel przetwarzania zgodnie z Art. 17 RODO, dla których wsparciem będzie zdefiniowanie zastosowanie w Systemie rozwiązań odnośnie kopii zapasowych (tworzenie, przechowywanie i odtwarzanie), ochrony kryptograficznej, ochrony przed złośliwym oprogramowaniem.
5. Opracowanie zestawu polityk, procedur i instrukcji dla grupy danych osobowych.
6. Wykorzystanie środków technicznych i organizacyjnych pozwalających spełnić wymagania art. 33 i 34 RODO dotyczących monitorowania, wykrywania, rejestrowania i raportowania naruszeń danych osobowych między innymi poprzez wykorzystanie:
   a. Systemów klasy SIEM do monitorowania i analizy wszelkich incydentów bezpieczeństwa.
   b. Systemów klasy DLP (ang. *Data Leak/Leakage/Loss Protection/Prevention*) integrowanych z systemem klasy SIEM i umożliwiającym dodatkowo monitorowanie wycieku danych, raportowanie o zdarzeniach a także systemową analizę podatności z tytułu naruszeń danych osobowych.
   c. Zapory firewall (Web Application Firewall; Database Firewall).

BDO-4. Wykonawca w procesie wytwórczym Systemu i E-Usługi jest zgodnie z RODO zobowiązany do stosowania zasady *Privacy By Design* polegającej na projektowaniu rozwiązania z poszanowaniem prawa do prywatności jego użytkowników/odbiorców co znajduje wymiar w następujących zasadach:

1. podejściu proaktywnym, nie reaktywnym, zaradczym, nie naprawczym;
2. prywatności jako ustawienia domyślnego w fazie projektowej (tzw. *Privacy by Default*);
3. prywatności włączonej w projekt (tzw. *Privacy Embedded Into Design*);
4. pełnej funkcjonalności (suma dodatnia, nie suma zerowa);
5. ochrony od początku do końca cyklu życia informacji;
6. widoczności i przejrzystości;
7. poszanowania dla prywatności użytkowników.

7.10.2. Bezpieczeństwo kodu

WBK-1. W ramach realizacji przedmiotu zamówienia, Wykonawca jest zobowiązany do realizacji analizy bezpieczeństwa kodu (ang. *SAST – Static Application Security Testing*) na etapie wytwarzania i weryfikacji kodu w zakresie:

1. **Przeglądów manualnych kodu** realizowanych przez zespoły programistyczne mających na celu zidentyfikowanie błędów związanych ze strukturą kodu, przyjętymi dobrymi praktykami, wewnętrznymi regulacjami, jak również zaimplementowanymi regułami biznesowymi i logiką aplikacji. Wykonywane są przez członków zespołu deweloperskiego, posiadających niezbędną wiedzę do przeprowadzenia takiej weryfikacji. Przeglądy powinny być przeprowadzane kilkukrotnie, powinny być też elementem planowania prac zgodnie z przyjętą metodyką projektowania Swoim zakresem mogą objąć cały wytwarzany kod.
2. **Automatycznej analizy statycznej kodu** mającej na celu zidentyfikowanie błędów związanych z konstrukcją kodu, definiowaniem zmiennych, wywołaniami metod, użyciem poszczególnych funkcji. Analiza statyczna może weryfikować kod w zakresie wystąpień wzorców wskazujących na prawdopodobieństwo wystąpienia błędu programistycznego jako Common Weakness Enumeration (CWE/SANS TOP 25– Weaknesses - most dangerous software errors) i OWASP Top 10. Analiza powinna być przeprowadzana kilkukrotnie na etapie wytwarzania oprogramowania, jak również na etapie testów bezpieczeństwa, będących etapem weryfikacji wytworzonego oprogramowania (testy penetracyjne). Swoim zakresem obejmuje cały wytwarzany kod. W związku z tym, że analiza przeprowadzana jest przy wykorzystaniu dedykowanych narzędzi, niezbędne jest opracowanie reguł i szablonów określających sposób weryfikacji dla zastosowanych języków programowania.
3. **Przeglądów manualnych kodu realizowanych przez zespół bezpieczeństwa** mających na celu przeprowadzenie dodatkowej weryfikacji obszarów, w których zidentyfikowano istotne błędy w ramach automatycznej analizy statycznej i testów penetracyjnych. Ma to na celu potwierdzenie potencjalnych błędów (poprzez eliminację „*false positives*") mogących mieć wpływ na bezpieczeństwo funkcjonowania systemu lub też na obniżenie skuteczności zastosowanych mechanizmów bezpieczeństwa.

WBK-2. Zakres przeglądów manualnych kodu realizowanych przez zespoły programistyczne będzie indywidualnie planowany w ramach przyjętej metodyki projektowania. Zebrane wyniki będą wykorzystywane na bieżąco przez zespoły programistyczne. Nie będą tworzone dodatkowe artefakty w postaci raportów z przeglądów.

WBK-3. Analiza statyczna kodu będzie realizowana jako element „*continuous integration*", przy wsparciu zespołu bezpieczeństwa oraz na zakończenie prac programistycznych, stanowiąc element testów bezpieczeństwa. Na tej podstawie Wykonawca opracuje raport zawierający między innymi listę zidentyfikowanych błędów lub podatności, poziom ich krytyczności oraz rekomendacje związane ze sposobem ich usunięcia.

WBK-4. Przegląd manualny kodu realizowany przez zespół bezpieczeństwa będzie stanowił uzupełnienie automatycznej analizy statycznej kodu. Uzyskane informacje o potwierdzonych błędach i podatnościach zostaną dołączone do ww. raportu z analizy statycznej kodu. Powyższa analiza powinna uwzględniać rozwiązania eliminujące lub znacząco zmniejszające podatność projektowanego systemu na ataki i być oparta na dobrych praktykach w zakresie bezpiecznego kodowania takimi jak CVE, CERT, MITRE CWE i ująć aktualne trendy w wektorach ataku.

7.10.3. Testy penetracyjne

Testy penetracyjne nie wchodzą w zakres niniejszego zamówienia. Zamawiający podaje założenia dla testów penetracyjnych, które zostaną zrealizowane przez podmiot wskazany przez Zamawiającego.

ZTP-1. Testy zostaną przeprowadzone zgodnie ze standardami testowania bezpieczeństwa, dla przykładu:

1. Open Web Application Security Project (OWASP) Web Security Testing Guide, Application Security Verification Standard,
2. Open Source Security Testing Methodology Manual (OSSTMM),
3. Penetration Testing Execution Standard (PTES).

ZTP-2. Skany podatności zostaną realizowane automatycznie lub w sposób dalece zautomatyzowany (przy użyciu specjalistycznego oprogramowania), uzupełnione testami penetracyjnymi uwzględniającymi wyniki skanowania.

ZTP-3. Zamawiający przewiduje objęcie testami penetracyjnymi elementów Systemu i E-Usługi w podziale na dwie grupy:

1. **testy aplikacji** – przeprowadzane w środowisku zbieżnym z produkcyjnym, mające zidentyfikować podatności możliwe do wykorzystania w trakcie użytkowania aplikacji. W ramach testów wykorzystywane będą narzędzia wspierające proces testowania (testy półautomatyczne). W ramach tych działań przewidywane są dwa podejścia, pierwsze „Gray Box" (na podstawie dostarczonej dokumentacji projektowej i przekazanej wiedzy od zespołu projektowego) prowadzone z wewnątrz, drugie „Black Box" prowadzone z zewnątrz.
2. **testy infrastruktury** – przeprowadzane w środowisku produkcyjnym, mające na celu zweryfikowanie poprawności instalacji i konfiguracji mechanizmów bezpieczeństwa infrastruktury sprzętowo-programowej, w tym:
   a. urządzeń sieciowych, serwerów oraz macierzy, systemów operacyjnych;
   b. usług sieciowych, aplikacji serwerowych;
   c. baz danych;
   d. zewnętrznych komponentów bezpieczeństwa;
   e. serwerów firewall, urządzeń HSM.

ZTP-4. W wyniku testów penetracyjnych zostanie opracowany raport zawierający między innymi listę zidentyfikowanych błędów i podatności, ich poziom krytyczności (istotności) oraz rekomendacje związane ze sposobem ich usunięcia.

ZTP-5. Wykonawca jest zobowiązany do usunięcia wykrytych w ramach testów penetracyjnych błędów i podatności.

8. Wymagania w zakresie Analizy Przedwdrożeniowej

WAP-1. Analiza Przedwdrożeniowa zawiera:

1. opis planowanych operacji przetwarzania danych osobowych w ramach budowanego Systemu i E-Usługi,
2. ocenę ich niezbędności oraz proporcjonalności w stosunku do celów realizowanych przez budowany System i E-Usługę,
3. ocenę ryzyka naruszenia praw lub wolności osób których dane dotyczą, a także środki planowane w celu zaradzenia temu ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych.

Analiza Przedwdrożeniowa musi zostać przygotowana w sposób przejrzysty z jasnym podziałem na elementy wymagane w przedmiocie zamówienia. W ramach analizy muszą być opisane w szczególności:

1. Projekt Systemu zawierający:
    a. Opis koncepcji budowy Systemu;
    b. Architekturę budowanego Systemu (architekturę fizyczną, logiczną, z podziałem na moduły funkcjonalne);
    c. Opis sposobu realizacji wszystkich wymagań wynikających z OPZ poprzez umieszczenie szczegółowego opisu sposobu realizacji w stosunku do każdego wymagania (przedstawiony w formie tabelarycznej z uwzględnieniem numeracji wymagań), przy czym powielenie treści wymagania nie może być opisem sposobu jego realizacji;
    d. Opis sposobu integracji z infrastrukturą Zamawiającego;
    e. Opis sposobu prezentacji danych/integracji z innymi systemami
    f. Opis koncepcji zbierania, walidacji i publikacji gromadzonych danych,
2. Przygotowanie prototypów interfejsu Użytkownika wraz zaznaczonymi interakcjami oraz opisem przepływu ekranów. Prototypy należy przygotować co najmniej dla kluczowych elementów budowanego Systemu:
    a. strona główna budowanego Systemu pozwalająca na dostęp do komponentów systemu,
    b. logowanie do systemu,
    c. okno dla wszystkich grup użytkowników z uwzględnieniem statusu zalogowany i niezalogowany,
    d. walidowania danych,
    e. eksportu danych,
    f. modułu administratora
3. Opis sposobu integracji Systemu z posiadanymi przez Zamawiającego systemami np.: WSO2IS/CSU, AD, oraz z próbnikami konsumenckimi i sieciowymi:
4. Przygotowanie wstępnych scenariuszy testowych (w tym automatycznych) obejmujących zakresem wszystkie (w tym wydajności, bezpieczeństwa, itp.) funkcjonalności opisane w SWZ i służących do przeprowadzenia przez Zamawiającego testów akceptacyjnych budowanego Systemu;
5. Szczegółowy harmonogram realizacji przedmiotu Umowy z zaznaczeniem kamieni milowych;
6. Analizy systemowe;
7. Fizyczna struktura danych;
8. Szczegółowy model danych gromadzonych w budowanym Systemie;
9. Administracja;
10. Bezpieczeństwo;

11. Dostępność;
12. Skalowalność rozwiązania;
13. Wydajność;
14. Technologia;
15. Ryzyka projektowe wraz z informacją o sposobie monitorowania i rejestrowania ryzyka, rodzaju działań jakie zostaną podjęte w przypadku wystąpienia ryzyka i określenie budżetu ryzyka;
16. Szanse projektowe;
17. Przyszłe możliwości rozwoju budowanego Systemu;
18. Opis w zakresie wymaganej infrastruktury teleinformatycznej, która zostanie dostarczona w ramach postępowania.

Dokument analizy musi być przygotowany zgodnie z wymaganiami dla dokumentacji wskazanymi w rozdziałach 8 i 11.

9. Wymagania w zakresie scenariuszy testowych i testów

Scenariusze testowe i testy obejmują:

1) oprogramowanie i infrastrukturę w części poza pomiarowej
2) oprogramowanie i urządzenia w części pomiarowej

ST-1. Wykonawca przygotuje i dostarczy w ramach Analizy Przedwdrożeniowej scenariusze testowe w celu sprawdzenia prawidłowości działania e-usługi z uwzględnieniem wymagań jakościowych:

a. System SMJI ma umożliwiać równoczesną pracę i możliwość wykonania pomiarów co najmniej 4000 użytkowników
b. Generowanie raportu z wykonanego pomiaru będzie zapewnione z poziomem jakości określonym poprzez:
    a. Czas wygenerowania raportu o objętości do 5 stron < 5 sek
    b. Czas wygenerowania raportu o objętości powyżej 5 stron < 20 sek.
c. Możliwość zapisania wygenerowanego raportu lokalnie przez użytkownika w formacie min. pdf.
d. System powinien poinformować użytkownika dokonującego pomiaru o braku komunikacji z próbnikiem (?)
e. Obsługa następujących przeglądarek internetowych: Microsoft Edge, Mozilla Firefox, Google Chrome, Opera, Apple Safari, w wersjach objętych wsparciem ich dostawców w dniu przekazania e-usługi do odbioru lub w wersjach nowszych.

ST-2. Scenariusze testowe muszą być pogrupowane i uporządkowane z uwzględnieniem kolejności wykonywania wynikającej z logiki działania Systemu.

ST-3. Scenariusz testowy musi zawierać w szczególności:

a. Unikalny numer,
b. Unikalną nazwę nawiązującą do testowanej funkcjonalności,
c. Opis sprawdzanych funkcjonalności,

d. dane wejściowe: opis danych wejściowych i warunków wstępnych niezbędnych do wykonania testu, numery scenariuszy, które muszą być wykonane wcześniej, aby bieżący scenariusz mógł być przeprowadzony poprawnie,
e. Kroki testowe: kolejno następujące po sobie akcje użytkownika i odpowiedzi Systemu,
f. Oczekiwany rezultat: opis końcowego rezultatu, spodziewanego po prawidłowym wykonaniu czynności testowych
g. Opis błędów - w przypadku wystąpienia błędów podczas realizacji scenariuszy należy opisać działanie Systemu, gdzie zostaną zalogowane i wyświetlone komunikaty błędów a także jaki będzie format wiadomości z informacjami o błędach.

ST-4. Scenariusze testowe będą podlegały aktualizacji zgodnie z cyklem wytwarzania Systemu.

ST-5. Scenariusze testowe muszą być aktualizowane w ramach Usługi Wsparcia i Rozwoju, niezwłocznie po dokonaniu zmian w Systemie.

ST-6. Wykonawca zobowiązuje się do aktualizacji dokumentacji zawierającej scenariusze testowe w sposób określony w Umowie.

ST-7. Zamawiający może przeprowadzić testy eksploracyjne i inne dodatkowe testy Systemu.

ST-8. Wymagania szczegółowe do testów Systemu:

a. Testy modułowe – przeprowadzane przez Wykonawcę
   i. Kod testów i dane testowe muszą być każdorazowo przekazywane Zamawiającemu wraz z wersją przekazywanego oprogramowania;
   ii. Muszą być uruchamiane dla każdej właściwej wersji kodu przekazywanej przez Wykonawcę;
   iii. Wykonawca każdorazowo zobowiązany jest do przekazania Zamawiającemu raportu z testów modułowych;
   iv. Przekazany raport z testów modułowych musi potwierdzać zakończenie testów z wynikiem pozytywnym;
b. Testy integracyjne – przeprowadzane przez Wykonawcę
   i. Muszą pokrywać wszystkie interfejsy wykorzystywane w komunikacji pomiędzy podsystemami/modułami/komponentami Systemu,
   ii. Muszą pokrywać wszystkie interfejsy wykorzystywane w komunikacji z systemami zewnętrznymi z którymi System zostanie zintegrowany,
   iii. Muszą być wykonywane dla każdej właściwej wersji Systemu przekazywanego przez Wykonawcę,
   iv. Wykonawca każdorazowo zobowiązany jest do przekazania Zamawiającemu raportu z testów integracyjnych;
   v. Przekazany raport z testów modułowych musi potwierdzać zakończenie testów z wynikiem pozytywnym
c. Testy regresyjne - przeprowadzane przez Wykonawcę
   i. Muszą być wykonane po każdej aktualizacji Systemu,
   ii. Wykonawca każdorazowo zobowiązany jest do przekazania Zamawiającemu raportu z testów regresyjnych,
d. Testy systemowe – przeprowadzane przez Wykonawcę

i. Muszą pokrywać wszystkie wymagania funkcjonalne i niefunkcjonalne Systemu,
ii. Muszą być uruchamiane dla każdej właściwej wersji kodu przekazywanej przez Wykonawcę i każdorazowo uwzględniać testy regresji,
iii. W przypadku braku możliwości wykonania testów integracji Systemu z systemami zewnętrznymi, Wykonawca dostarczy komponenty symulujące pracę systemów zewnętrznych,
iv. Wykonawca każdorazowo zobowiązany jest do przekazania Zamawiającemu raportu z testów systemowych,
v. Wykonawca każdorazowo zobowiązany jest do przekazywania skryptów testów systemowych.

e. Testy akceptacyjne – przeprowadzane przez Zamawiającego w celu potwierdzenia prawidłowości działania Sytemu z uwzględnieniem wszystkich wymagań funkcjonalnych i niefunkcjonalnych oraz przypadków użycia.
f. Testy bezpieczeństwa – przeprowadzane przez Wykonawcę w celu potwierdzenia prawidłowości działania Systemu pod kątem jego bezpieczeństwa. Po zakończeniu testów bezpieczeństwa przed przekazaniem Systemu do odbioru, Wykonawca przekaże Zamawiającemu raport z testów bezpieczeństwa Systemu:
    i. System ma być zgodny z wytycznymi zawartymi w metodyce OWASP Testing Guide w wersji 5 oraz w dokumencie OWASP ASVS 4.0 (Application Security Verification Standard).
    ii. System ma być zgodny z wytycznymi zawartymi w standardzie PTES (Penetration Testing Execution Standard) w zakresie infrastruktury.
g. Zakres testów bezpieczeństwa:
    i. Testy konfiguracji (W trakcie testów powinny być sprawdzane m.in.:),
        1. mechanizmy kryptograficzne stosowane w ramach aplikacji i infrastruktury (stosowanie protokołu SSL/TLS),
        2. ustawienia dostępu do bazy danych,
        3. obsługa plików o różnych rozszerzeniach,
        4. istnienie na serwerze poprzednich wersji lub kopii zapasowych aplikacji,
        5. istnienie interfejsów do zarządzania oraz próby dostępu do nich,
        6. typy obsługiwanych żądań http,
    ii. Testy mechanizmów zarządzania sesją (W trakcie testów powinny być sprawdzane m.in.:),
        1. weryfikacja schematu zarządzania sesją,
        2. obsługa parametrów sesji przez aplikację (pliki Cookies),
        3. próby podszywania się pod zalogowanego Użytkownika,
        4. próby wstrzykiwania innych parametrów sesji,
        5. odporność na ataki typu Session Fixation,
        6. weryfikacja jawności parametrów sesji,

7. weryfikacja mechanizmów wygaszania sesji,
8. weryfikacja istnienia podatności typu CSRF (Cross Site Request Forgery)

iii. Testy walidacji danych i możliwości wstrzykiwania kodu (W trakcie testów powinny być sprawdzane m.in.:),

1. weryfikację istnienia podatności Cross-Site Scripting (Reflected, Stored),
2. analizę podatności typu HTTP verb pollution/tampering,
3. analizę pod kątem istnienia podatności SQL Injection, w tym blind, time-delay, Boolean, database specific,
4. weryfikację pod kątem podatności typy OS command injection,
5. weryfikację pod kątem podatność klasy serwer side injection,
6. analizę pod kątem istnienia podatności XML/XPATH Injection,
7. weryfikację pod kątem istnienia podatności typu local/remote file inclusion,
8. analizę pod kątem istnienia błędów typu buffer overflow, heap overflow, format string

iv. Testy mechanizmów obsługi błędów,

1. W trakcie testów powinny być sprawdzane komunikaty o błędach jakie zostaną wywołane przez wprowadzanie różnych wartości parametrów oraz tzw. stack traces

v. Testy po stronie klienta (przeglądarki),

1. weryfikacja podatności typu DOM based Cross Site Scripting,
2. weryfikacja podatności typu HTML Injection,
3. weryfikacja podatności typu Client Side URL Redirect,
4. weryfikacja podatności typu Client Side Resource Manipulation,
5. analiza zastosowanej polityki Cross Origin Resource Sharing,
6. weryfikacja podatności typu Clickjacking

vi. Weryfikacja mechanizmów kryptograficznych pod kątem możliwości użycia słabych algorytmów,

1. weryfikację możliwości użycia słabych algorytmów kryptograficznych (szyfrów symetrycznych, asymetrycznych, funkcji skrótu),
2. analizę pod kątem ujawniania poufnych informacji przez aplikację

h. Testy wydajnościowe – przeprowadzane przez Wykonawcę w celu potwierdzenia spełnienia wymagań wydajnościowych Systemów. Po zakończeniu testów wydajności przed przekazaniem Systemu do odbioru, Wykonawca przekaże Zamawiającemu raport z testów bezpieczeństwa Systemu.

i. Wykonawca wykona testy wydajnościowe Systemu dwa razy. Pierwszy test przed przekazaniem Systemu do odbioru. Drugi w terminie uzgodnionym z Zamawiającym w okresie pomiędzy Odbiorem Końcowym a końcem okresu Gwarancji.

ii. Po zakończeniu testów wydajnościowych Wykonawca przekaże Zamawiającemu raport z testów wydajnościowych,

iii. Testy wydajnościowe muszą obejmować co najmniej:

1. Realizacja testów obejmie wykonanie zaproponowanego i odpowiedniego rodzaju testu wydajnościowego przy pomocy dedykowanych skryptów testowych, opisanych w metodyce, odzwierciedlających konkretne scenariusze wykorzystania aplikacji przez Użytkownika lub żądania generowane w ramach integracji pomiędzy systemami.
2. Skrypty służące do realizacji takiego testu mają zostać stworzone przy pomocy dedykowanego narzędzia Open Source wspierającego testy wydajnościowe i polegają na nagraniu ruchu generowanego i odbieranego przez aplikację, a następnie – odpowiednio sparametryzowane – uruchamiane będą wielokrotnie, symulując wykorzystywanie aplikacji przez zdefiniowaną liczbę Użytkowników.
3. Wykonawca w swojej metodyce ma zaproponować i uzasadnić liczbę cykli wykonywania testu i iteracji, przy czym plan musi uwzględniać różne cele kolejnych cykli/iteracji – np.: weryfikacja wydajności Systemu po implementacji poprawek, weryfikacja wydajności Systemu po implementacji poszczególnych zmian, badanie wydajności Systemu przy zmieniającym się obciążeniu.

iv. Testy wydajnościowe muszą polegać na weryfikacji wydajności Systemu po stronie serwera/ów aplikacji i/lub bazy danych, jak i na badaniu czasu reakcji samego interfejsu graficznego użytkownika w czasie obciążenia Systemu. Wykonawca do tych pomiarów musi użyć własnych dodatkowych narzędzi Open Source.

10. Wymagania w zakresie sposobu realizacji zamówienia

WRP-1. Metodyka *waterfall* zostanie zastosowana na poziomie organizacji projektu oraz pilnowania realizacji harmonogramu ramowego, metodyka agile do iteracji działań, aż wszystkie przypadku użycia zostaną rozwiązane.

WRP-2. Planowanie, projektowanie i definiowane wymagań należy wykonać z pomocą *waterfall*, ale rozwój i testowanie w krótkich sprintach (2-tyg) z pomocą agile.

11. Wymagania w zakresie dokumentacji

WD-1. Każda z procedur w dokumentacji musi zawierać co najmniej następujące informacje:

1. Identyfikator procedury,
2. Nazwa procedury,
3. Wersja procedury,
4. Data początku obowiązywania procedury,
5. Cel realizacji procedury,
6. Warunki uruchomienia procedury,

7. Warunki zakończenia realizacji procedury – opis efektu końcowego realizacji procedury,
8. Odpowiedzialność - określenie osób/ról ponoszących odpowiedzialność za stosowanie procedury,
9. Wykaz dokumentów związanych - wykaz dokumentów związanych, w tym dokumentów opisujących procedury zależne,
10. Wykaz aplikacji wspomagających wykonywanie procedur (np. system monitorowania),
11. Tryb postępowania - opis kolejnych kroków procedury.

WD-2. Wymagania ogólne dotyczące dokumentacji:

1. Wykonawca dostarczy dokumentację, korzystając z funkcjonalności Confluence pakietu Atlassian do którego dostępy przekaże Wykonawcy Zamawiający.
2. Wykonawca będzie dokonywał zmian i aktualizacji dokumentacji, o ile takie zmiany będą konieczne z uwagi na wprowadzane modyfikacje Systemu lub wykryte błędy i nieprawidłowości w jego działaniu.
3. Zaktualizowana dokumentacja będzie dostarczana Zamawiającemu wykorzystując funkcjonalność Confluence, nie później niż w terminie określonym w Umowie.

11.1. Dokumentacja Użytkownika

WDU-1. Wykonawca przygotuje instrukcję użytkownika, która będzie zawierać szczegółowy opis wszelkich funkcjonalności i właściwości dostarczonego Systemu. Treść instrukcji użytkownika będzie pozwalać na poprawną eksploatację i samodzielną naukę obsługi Systemu.

WDU-2. Instrukcja będzie zawierać co najmniej wyszczególnione poniżej elementy:

a. opis sposobu uruchomienia Systemu i zalogowania użytkownika,
b. opisy poszczególnych elementów ekranów (okien) Systemu,
c. opis wszystkich funkcji menu Systemu oraz funkcjonalności interfejsu użytkownika,
d. opis funkcjonalności Systemu,
e. opis procesu przygotowania zadań pomiarowych, wykonywania zadań pomiarowych, zapisu i przeglądania wyników w tym wyników archiwalnych,
f. wykaz komunikatów błędów generowanych przez System wraz z ich opisem, możliwymi przyczynami oraz propozycjami sposobu ich eliminacji przez użytkownika.

WDU-3. Wykonawca przygotuje skróconą instrukcję instalacji próbnika konsumenckiego, która powinna być dołączona do każdego próbnika w formie ulotki.

11.2. Dokumentacja Techniczna

WDT-1. W dokumentacji technicznej muszą być zawarte opisy wszelkich cech, właściwości i funkcjonalności pozwalających na poprawną z punktu widzenia technicznego eksploatację Systemu. W szczególności dokumentacja ta będzie zawierać:

a. Opis architektury Systemu obejmujący:
    i. architekturę tzn. schemat i opis powiązań logicznych poszczególnych komponentów i ich rolę w architekturze,
    ii. architekturę tzn. schemat i opis integracji Systemu z innymi systemami,

iii. parametry techniczne i konfiguracyjne urządzeń pomiarowych (próbników sieciowych i konsumenckich), Głównego Serwera Systemu, Głównego Serwera Testowego, Serwerów Testowych,

b. Opis konfiguracji Systemu obejmujący dane konfiguracyjne, w szczególności: wersje Systemu, katalog instalacyjny, położenie plików konfiguracyjnych, pierwotne parametry konfiguracyjne i zmodyfikowane w procesie instalacji, lokalizacji plików logów, lokalizację i opis innych kluczowych plików i katalogów, parametry instancji. Dane, o jakich mowa wyżej będą pogrupowane odrębnie dla:

i. Infrastruktury IT,

ii. urządzeń pomiarowych,

c. Procedury eksploatacji serwerów obejmujące w szczególności:

i. tworzenie kopii bezpieczeństwa systemu operacyjnego i kopii zapasowych oraz odtwarzanie z ww. kopii wszystkich komponentów aplikacji i środowiska (bazy danych, komponenty serwera aplikacji, klienta itp.),

ii. odtworzenie systemu po katastrofie (disaster recovery),

iii. procedury opisujące kolejne kroki pozwalające na bezpieczne zatrzymanie/uruchomienie poszczególnych elementów Systemu,

iv. aktualizację Systemu, w szczególności procedury lub instrukcje instalacji, reinstalacji, deinstalacji oraz aktualizacji obejmujące szczegółowy opis postępowania w przypadku tworzenia lub zmian w środowisku jeśli wykorzystywane są procedury innych dostawców dla standardowych komponentów (np. baz danych) wystarczy wskazać w dokumentacji szczegółowe odniesienie do procedur standardowych właściwych dla tych komponentów,

v. procedury backupowe obejmujące zalecany tryb backupu aplikacji i elementów infrastruktury software'owej, oraz zakres danych podlegających backupowi. Procedury odtworzeniowe, muszą w szczególności opisywać sposób odtworzenia funkcjonalności aplikacji i elementów infrastruktury software'owej w przypadku błędu lub awarii,

vi. opis (w postaci procedur, instrukcji, harmonogramów) wszystkich czynności administracyjnych dla Systemu.

11.3. Dokumentacja Instruktażowa

WDI-1. Wykonawca przygotuje krótkie pisemne instruktaże oraz filmy instruktażowe wraz z profesjonalnym lektorem, etykietami wyświetlanymi na tle filmu, co najwyżej pięciominutowe (każdy), które będą prezentować, w jaki sposób należy korzystać z funkcjonalności Systemu, w szczególności:

a. W jaki sposób poprawnie podłączyć próbnik wykorzystywany do pomiaru,

b. Utworzenie konta użytkownika w systemie,

c. Logowanie/wylogowywanie w Systemie,

d. W jaki sposób wykonać pomiar testowy,

e. W jaki sposób zapisać lokalnie wynik pomiaru,

f. W jaki sposób sięgnąć do pomiarów archiwalnych,

WDI-2. Wykonawca przygotuje propozycje scenariuszy do tych instruktaży oraz filmów instruktażowych, które podlegać będą akceptacji Zamawiającego. Filmy instruktażowe Wykonawca opracuje w jakości co najmniej 480p oraz w postaci plików mp4.

WDI-3. Pisemne instruktaże oraz filmy instruktażowe będą przygotowane po zakończeniu testów akceptacyjnych i aktualizowane w całym okresie gwarancji i świadczenia usług wsparcia w przypadku zmian w działaniu Systemu.

11.4. Dokumentacja Administratora

Dokumentacja Administratora Systemu oraz Dokumentacja Administratora E-Usługi musi zawierać:

WDA-1. Zestaw dokumentacji szczegółowo opisujących zastosowane rozwiązania zapewniające spełnienie wymagań ogólnych (zgodnie z wymaganiami prawa) oraz specyficznych zamawiającego dotyczących bezpiecznej eksploatacji.

WDA-2. Opis zastosowanych mechanizmów logowania zdarzeń, śladu audytowego oraz kontroli i monitorowania działań w Systemie i E-Usłudze w tym wszelkich prób naruszenia zasad bezpieczeństwa.

WDA-3. Opis funkcjonalności, interfejs oraz zasady zarządzania kontami użytkowników i usług oraz uprawnieniami poszczególnych ról, profili, kont.

WDA-4. Opis sposobu realizacji wymagań wynikających z obowiązujących przepisów o ochronie danych osobowych.

WDA-5. Opis zabezpieczeń interfejsów oraz opis metod zapewnienia poufności i kontrolowalności tych kanałów przepływu informacji, jeśli aplikacja wykorzystuje jakiekolwiek mechanizmy wymiany informacji z innymi systemami.

WDA-6. Opisy instalacji, konfiguracji i parametryzacji oprogramowania zastosowanego przy budowie Systemu i E-Usługi (stos technologiczny) z uwzględnieniem:

1. Zestawienia wersji zastosowanego oprogramowania, w tym oprogramowania systemowego, narzędziowego i aplikacyjnego.
2. Zestawienia parametrów systemu operacyjnego i oprogramowania narzędziowego, które są modyfikowane względem wartości domyślnych.

WDA-7. Opisy instalacji, konfiguracji i parametryzacji oprogramowania aplikacyjnego Systemu i E-Usługi (stos technologiczny) z uwzględnieniem:

1. Zestawienia parametrów oprogramowania aplikacyjnego z podaniem:
   a. Definicji i opisu parametru oraz jego znaczenia.
   b. Wartości parametru (oraz minimalnej i maksymalnej wartości parametru).
   c. Zestawienia i opisu plików konfiguracyjnych zawierających standardową konfigurację po uruchomieniu.
2. Zestawienia zdarzeń, które skutkują zapisaniem komunikatów w logach poszczególnych komponentów Systemu. Komunikaty generowane przez aplikacje Systemu i E-Usługi muszą uwzględnić co najmniej następujące informacje:
   a. Identyfikator zdarzenia wykorzystywany w logach pozwalający na zidentyfikowanie go w dokumentacji.
   b. Opis i wyjaśnienie zdarzenia.

WDA-8. Opis działań, które muszą zostać zrealizowane przy wystąpieniu komunikatu.

WDA-9. Komplet procedur administracyjnych uwzględniających:

1. Pełną instalację Systemu i uruchomienie E-Usługi,
2. Uruchomienie i zatrzymanie komponentów Systemu i E-Usługi,
3. Opis metod zmian parametrów komponentów Systemu i E-Usługi,
4. Kontrolę poprawności działania Systemu i E-Usługi względem przyjętych parametrów wydajnościowych i jakościowych,
5. Zarządzanie uprawnieniami,
6. Wykonanie i odtworzenie kopii zapasowej z uwzględnieniem polityki bezpieczeństwa Zamawiającego,
7. Postępowanie i naprawę Systemu i E-Usługi w przypadku awarii.

WDA-10. Polityki i procedury dla procesów cyklicznych:

1. Bieżących aktualizacji komponentów oprogramowania pod kątem podatności, aktualności wersji, polityki uwierzytelniania, tworzenia (złożoności) i zmiany haseł, kontroli i hierarchii dostępu, bezpieczeństwa i archiwizacji danych.
2. Kontroli efektywności i kompleksowości mechanizmów redundancji, dostępu do oprogramowania systemowego, aktualizacje oprogramowania systemowego pod kątem usuwania luk i aktualizacji jego wersji, zapewnienia pełnej kontroli nad dostępem do fizycznych komponentów architektury.

11.5. Dokumentacja Testowa

DT-1. Wykonawca jest zobowiązany do opracowania i przedstawienia do akceptacji Zamawiającego:

a. Planów testów dla każdego z typów realizowanych testów:
   i. Testy modułowe,
   ii. Testy integracyjne,
   iii. Testy systemowe w tym regresji,
   iv. Testy akceptacyjne,
   v. Testy bezpieczeństwa,
   vi. Testy wydajności,
b. Scenariuszy testowych dla wszystkich typów testów
c. Zestawienia przypadków testowych
d. Danych testowych dla poszczególnych przypadków

DT-2. Plan Testów przygotowany przez Wykonawcę musi zawierać co najmniej następujące informacje:

a. Słownik pojęć,
b. Wprowadzenie i cel testów,
c. Przedmiot i zakres testów,
d. Zestawienie scenariuszy testowych wraz z pokryciem wymagań przez poszczególne scenariusze,
e. Zestawienie przypadków testowych dla poszczególnych scenariusz wraz z opisem pól,
f. Kryteria rozpoczęcia testów,

g. Kryteria zakończenia testów,
h. Zasady raportowania i cykl życia scenariuszy testowych,
i. Lista narzędzi testowych,
j. Zdefiniowanie ograniczeń (np. dostępność zasobów wymaganych do przeprowadzenia testów, ograniczenia wynikające z harmonogramu),
k. Kategorie incydentów,
l. Harmonogram testów,
m. Opis środowiska testowego,
n. Opis struktury Zespołu testowego,
o. Opis zakresu danych testowych, dostarczanych przez Wykonawcę dla poszczególnych scenariuszy testowych.

DT-3. Scenariusze testowe muszą zawierać co najmniej następujące informacje:

a. Konstrukcja scenariuszy testowych musi zapewniać możliwość ich wykonania przez osoby wskazane przez Zamawiającego (osoby niebędące członkami Zespołu Wykonawcy), posiadające kwalifikacje w zakresie testowania aplikacji.
b. Konstrukcja scenariuszy testowych musi zapewniać możliwość zweryfikowania pokrycia wymagań i przypadków użycia. W szczególności musi być możliwe zidentyfikowanie:
    i. Wymagań (funkcjonalnych i niefunkcjonalnych) weryfikowanych przez scenariusz testowy,
    ii. Przypadków użycia weryfikowanych przez scenariusz testowy;
c. Dokument scenariusza testowego musi uwzględniać:
    i. Identyfikator scenariusza,
    ii. Warunki wejściowe – lista warunków, jakie muszą być spełnione, aby można było rozpocząć wykonanie ST,
    iii. Określenie zakresu danych testowych,
    iv. Listę przypadków testowych wchodzących w skład scenariusz testowego;
d. Dokument przypadku testowego musi uwzględniać:
    i. Uporządkowany i jednoznaczny zestaw kroków wykonywanych przez testera,
    ii. Opis oczekiwanego wyniku po wykonaniu poszczególnych kroków,
    iii. Dodatkowe weryfikacje, które powinny zostać wykonane po zrealizowaniu danego scenariusza (np. czy dokonał się właściwy zapis w logu aplikacji);
e. Skrypty testowe do testów automatycznych
    i. Wykonawca zobowiązany jest do przygotowania skryptów do testów automatycznych, które będą wykorzystywane w czasie testów funkcjonalnych i testów regresji. Wraz kodami testów Wykonawca dostarczy dane testowe wymagane do ich realizacji.
    ii. Testy automatyczne będą uruchamiane z poziomu narzędzi do testów automatycznych wchodzących w skład środowiska CI.
    iii. Zakres testów będzie obejmował główne przypadki użycia, jednak nie może to być mniej niż 40% wszystkich zidentyfikowanych przypadków użycia dla Użytkowników Zewnętrznych i 40% wszystkich zidentyfikowanych przypadków użycia dla Użytkowników Zewnętrznych.

iv. Wszystkie testy muszą obejmować test ścieżki głównej i co najmniej jednej ścieżki alternatywnej.

11.6. Kody źródłowe

WDK-1. Wykonawca będzie wgrywał do repozytorium, które będzie w posiadaniu Zamawiającego, całą dokumentację łącznie z kodami źródłowymi komponentów Systemu każdorazowo przed instalacją nowej wersji Systemu, jego hot-fix'a lub rozszerzenia. Repozytorium musi być zorganizowane w sposób jednoznacznie określającym kolejne wydania oraz zakres zmian w stosunku do poprzedniej wersji. Repozytorium musi zawierać kody źródłowe wszystkich komponentów programowych Systemu, w tym: procedury, pliki konfiguracyjne, skrypty itd., wszystkie aktualizacje i poprawki, a także wdrożenia w ramach rozwoju wprowadzane w toku trwania umowy będą miały odzwierciedlenie we wspomnianym repozytorium, będą udokumentowane i będą posiadać odpowiednie komentarze. Repozytorium będzie stanowiło źródło programów, skryptów, kodów, etc. niezbędnych w procesach instalacji lub modyfikacji/rozszerzenia Systemu będą wykorzystywane przez narzędzia automatyzujące te procesy.

WDK-2. Wykonawca zobowiązany jest do przekazania Zamawiającemu:

a. W zakresie kodu aplikacji:

i. aktualny kod aplikacji i jego skompilowane wersje w podziale na poszczególne komponenty Systemu, który umożliwiał będzie jego kompilację, o ile kod będzie kompilowany,

ii. aktualną dokumentację dla kodu źródłowego zawierającej minimum:

1. listę wszystkich klas i funkcji wraz z opisem parametrów wejściowych i wyjściowych,
2. listę bibliotek i kontrolek, wraz z ich wersjami,
3. przepływ danych pomiędzy poszczególnymi komponentami Systemu (w postaci diagramów) w tym szczegółowy wykaz operacji komunikacji z bazami danych,
4. przepływ danych pomiędzy poszczególnymi komponentami Systemu a innymi systemami z którymi nastąpi integracja,
5. instrukcje kompilowania kodów źródłowych (o ile będą kompilowane) oraz instrukcje instalacje wytworzonych komponentów w środowisku o programowania standardowego,
6. opis parametrów konfiguracyjnych komponentów Systemu.

b. W zakresie baz danych:

i. aktualnych skryptów umożliwiających utworzenie baz danych, tabel, widoków, synonimów, procedur składowanych i funkcji,

ii. aktualnej dokumentacji do baz danych, tabel, widoków, synonimów, procedur składowanych i funkcji,

iii. dokumentacja powinna zawierać minimum takie informacje jak: nazwy danych, typy, wartości domyślne, opis kluczy głównych i kluczy zewnętrznych, indexy, w przypadku procedur i funkcji wartości wejściowe i wyjściowe,

WDK-3. Zamawiający wymaga, by kod źródłowy Systemu był zarządzany zgodnie z wzorcem ciągłej integracji (Continuous Integration). Dlatego Wykonawca zobowiązany jest do skonfigurowania i utrzymywania w czasie trwania Umowy środowiska ciągłej integracji (Continuous Integration) z wykorzystaniem posiadanego przez Zamawiającego oprogramowania Jenkins i Bitbucket, które będzie uwzględniało następujący zestaw narzędzi:

a. Repozytorium kodu,
b. Automatyczne budowanie Systemu,
c. Testy statyczne kodu źródłowego oraz weryfikację zgodności formatowania kodu względem przyjętej konwencji formatowania kodu,
d. Testy automatyczne,
e. Repozytorium oprogramowania na potrzeby składowania binariów poszczególnych wersji Systemu oraz wykorzystywanych bibliotek.

WDK-4. Na podstawie Dokumentacji Technicznej Wykonawca przygotuje i wdroży procedury do:

a. Automatycznego budowania poszczególnych wersji Systemu,
b. Automatycznego uruchamiania testów jednostkowych i funkcjonalnych.

WDK-5. W celu przeprowadzenia procedury odbioru kodów źródłowych Wykonawca przy współudziale Zamawiającego dokona kompilacji przekazanego kodu źródłowego zgodnie z przekazaną instrukcją, a następnie dokona instalacji wytworzonych komponentów w środowisku testowym Oprogramowania również zgodnie z przekazaną instrukcją.

WDK-6. Kod źródłowy użytych komponentów Open Source nie może podlegać zmianom. Modyfikacji mogą podlegać jedynie:

a. błędnie działające fragmenty kodu, przy czym błąd musi zostać zgłoszony autorom komponentu wraz z poprawionym przez Wykonawcę fragmentem kodu,
b. inne fragmenty, kodu w przypadku uzasadnionej potrzeby i za zgodą Zamawiającego.

WDK-7. Wszelkie zmiany w funkcjonalności komponentów Open Source powinny być realizowane w formie modułów, rozszerzeń lub wtyczek.

12. Wymagania w zakresie instruktażu

<podział na odbiorców szkoleń, tylko personel Zamawiającego>

WI-1. Wykonawca przygotuje i przeprowadzi, w terminie określonym w Harmonogramie i w miejscu na terenie RP wskazanym przez Zamawiającego, instruktaż dotyczące obsługi Systemu dla pracowników Zamawiającego. Forma i zakres tematyczny instruktaży muszą zostać zaakceptowane przez Zamawiającego.

WI-2. Instruktaże powinny być przeprowadzone na minimum trzech poziomach: poziom użytkownika, poziom administratora biznesowego oraz poziom administratora technicznego,

WI-3. Maksymalna liczba uczestników:

a. 5 administratorów technicznych,
b. 5 administratorów biznesowych,
c. 20 użytkowników Warszawa, 30 użytkowników delegatur.

WI-4. Czas instruktażu: minimum 16h (2 dni) – dla każdego z trzech poziomów, przy czym

poszczególne poziomy będą realizowane w odrębnych instruktażach i niepokrywających się terminach.

WI-5. Wykonawca opracuje i przedstawi Zamawiającemu do akceptacji harmonogram instruktaży, obejmujący terminy realizacji wszystkich instruktaży oraz zakresy tematyczne.

13. Wymagania dotyczące poziomu świadczenia usług (SLA)

SLA-1. Zamawiający wymaga świadczenia przez Wykonawcę następujących usług:

a. Dostępności Systemu:
   i. Zakres usług dostępu do Systemu rozumiany jest jako realizacja przez System wszystkich funkcjonalności zgodnie z zatwierdzoną Dokumentacją oraz obowiązującym prawem.
   ii. Usługi dostępu do Systemu będą świadczone w trybie 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku, 366 dni w roku przestępnym.
   iii. W przypadku konieczności naprawy Błędów, naprawy będą realizowane przez całą dobę. W przypadku konieczności wprowadzania zmian innych niż mające na celu naprawę Błędów, Wykonawca dokona ich jedynie w oknach serwisowych wyznaczanych w godzinach od 20:00 do 7:00 lub w innych godzinach za zgodą Zamawiającego. Podczas trwania prac w czasie okna serwisowego Wykonawca zapewnia wyświetlanie Użytkownikom Systemu komunikatu o trwających pracach serwisowych oraz planowanym terminie ich zakończenia zaś na 24 godziny przed uruchomieniem okna serwisowego Wykonawca zapewni wyświetlenie komunikatu o planowanych pracach serwisowych oraz planowanym terminie ich zakończenia.
   iv. Dla zapewnienia wysokiej dostępności Systemu wykonawca zobowiązany jest do zastosowania modelu architektury, który zapewni niezawodność całego rozwiązania. W tym wypadku Zamawiający wymaga zastosowania redundancji komponentów Systemu we wszystkich jego warstwach.
   v. Komponenty Systemu w środowisku produkcyjnym muszą być uruchomione jako klastry serwerów działających w trybie wysokiej dostępności (HA).
   vi. W Systemie musi zostać zagwarantowana dostępność na poziomie nie mniejszym niż 98% w skali miesiąca.
b. Wydajności Systemu:
   i. System musi zapewnić skalowalność (na poziomie warstw front-end, back-end i warstwie bazodanowej) w zakresie wydajności i pojemności oraz dołączania dodatkowych Użytkowników oraz elementów infrastruktury sprzętowej.
   ii. System musi zapewniać równoległą obsługę Użytkowników. Wydajność Systemu musi zostać zapewniona przy jednoczesnym korzystaniu z Systemu przez:
      1. 40 użytkowników wewnętrznych (pracownicy UKE),
      2. 500 – zalogowanych użytkowników zewnętrznych (Przedsiębiorcy telekomunikacyjni, jednostki samorządu terytorialnego, przedsiębiorstwa użyteczności publicznej)
      3. 50 – użytkowników zewnętrznych (Pozostali, niezalogowani użytkownicy)

iii. Wydajność Systemu będzie weryfikowana w czasie testów wydajnościowych, które zostaną przeprowadzone przez Zamawiającego.

SLA-2. Pomiar u UK nie powinien być dłuższy niż 35 dni.

SLA-3. Pomiar powinien być na tyle długi, aby wykazać prędkość minimalną, maksymalną i zwykle dostępną.

SLA-4. Wyniki pomiarów będą synchronizowane na bieżąco, niezwłocznie po zakończeniu pomiaru.

14. Wymagania dotyczące gwarancji

WG-1. Wykonawca udzieli Gwarancji oraz będzie świadczył Usługi Wsparcia Systemu. Zgłoszenia w zakresie Gwarancji będą dokonywane za pośrednictwem funkcjonalności *Help-Desk*, a w przypadku braku takiej możliwości za pośrednictwem poczty elektronicznej na dedykowany adres mailowy Wykonawcy. W przypadku błędów zgłoszenie będzie zawierało co najmniej następujące informacje:

a. kategoria ujawnionego Błędu w działaniu Systemu,

b. opis nieprawidłowości w działaniu Systemu,

c. opis błędu raportowany przez System, o ile będzie dostępny;

WG-2. Wykonawca odpowiada za prawidłowe działanie całości Systemu i każdego jego elementu z osobna, zgodnie z wymaganiami określonymi w Umowie, w tym w szczególności w OPZ oraz w Analizie Przedwdrożeniowej.

WG-3. Wykonawca odpowiada za zachowanie integralności i ciągłości pracy Systemu, także w przypadku obsługi Błędów, instalacji Aktualizacji, jakichkolwiek poprawek lub innych zmian w Systemie, dokonywanych przez Wykonawcę w celu wdrożenia Systemu lub usunięcia Błędów.

WG-4. W ramach obsługi Błędów Systemu Wykonawca nie może usuwać jakichkolwiek danych aktualnych i archiwalnych, z wyjątkiem sytuacji uzgodnionych przez Wykonawcę i Zamawiającego w formie pisemnej pod rygorem nieważności.

WG-5. W ramach Gwarancji na System Wykonawca zapewni:

a. obsługę Błędów w Systemie, w terminach niżej określonych (Gwarantowany Czas Naprawy):

i. Błąd Krytyczny – Wykonawca zobowiązuje się określić przyczynę i usunąć błąd w nieprzekraczalnym terminie 2 dni robocze od zgłoszenia,

ii. Błąd Niekrytyczny – Wykonawca zobowiązuje się określić przyczynę i usunąć błąd w nieprzekraczalnym terminie 5 dni roboczych od zgłoszenia,

iii. Usterka – Wykonawca zobowiązuje się określić przyczynę i usunąć błąd w nieprzekraczalnym terminie 14 dni roboczych od zgłoszenia,

b. usuwanie Błędu Regresji – Wykonawca zobowiązuje się określić przyczynę Błędu Regresji usunąć go i uruchomić System w terminie 7 dni roboczych.

WG-6. Dokonując zgłoszenia w ramach Gwarancji, Zamawiający określa kategorię Błędu zgodnie z definicjami zawartymi w OPZ. Kategorię Błędu określa Zamawiający i jest to wiążące dla

Wykonawcy.

WG-7. Minimalny wymagany przez Zamawiającego okres gwarancji wynosi 12 miesięcy od dnia podpisania Protokołu Odbioru Końcowego.

WG-8. Dostarczona infrastruktura (serwery, macierze, półki dyskowe) powinna być objęta gwarancją producenta sprzętu równą pod względem długości z gwarancją systemu, realizowaną w trybie NBD z czasem reakcji 4 godzin, w miejscu instalacji sprzętu. Wykupiona gwarancja powinna umożliwiać zgłaszanie awarii w trybie 24x7.

Uszkodzone nośniki danych (dyski) pozostają u Zamawiającego.

WG-9. Próbniki sieciowe – standardowa procedura reklamacji 14 dni?

WG-10. Próbniki konsumenckie – standardowa procedura reklamacji 14 dni?

15. Wymagania dotyczące Usług Wsparcia

WUG-1. W ramach usługi Wsparcia, Wykonawca zapewni konfigurację, aktualizację i konserwację środowiska, polegającą w szczególności na:

a. bieżącej aktualizacji oprogramowania systemowego serwerów, serwerów aplikacyjnych i bazodanowych w trybie opisanym w pkt WUG-2 lit. c,
b. bieżącej aktualizacji mechanizmów tworzących kopie bezpieczeństwa w trybie opisanym w pkt WUG-2 lit c,
c. konsultacjach technicznych dla administratorów (technicznych i biznesowych) w trybie określonym w pkt. WUG-2 lit a,
d. rozwiązywaniu problemów technicznych związanych z Systemem w trybie określonym w pkt. WUG-2 lit. b,
e. wsparciu wiedzą w postaci realizacji usługi hotline, przy czym dostępność usługi hotline nie może być świadczona w wymiarze mniejszym niż w trybie określonym w pkt. WUG-2 lit.b,
f. zapewnieniu współpracy Systemu z innymi systemami Zamawiającego i systemami zewnętrznymi wymienionymi w Rozdziale 4, poprzez usuwanie każdego błędu integracji wynikającego z działania Systemu w terminie nie później niż 5 dni roboczych od zgłoszenia,
g. zapewnieniu nadzoru autorskiego obejmującego monitorowanie kierunków Rozwoju Systemu oraz doradztwo Zamawiającemu w zakresie rozwoju m.in. w zakresie funkcjonalności, bezpieczeństwa i wydajności, w terminie uzgodnionym z Zamawiającym, nie później niż 30 dni od zgłoszenia,
h. utrzymaniu i aktualizacji dokumentacji systemu w repozytorium wiedzy udostępnionym przez Zamawiającego za pomocą funkcjonalności *Confluence* pakietu *Atlassian*, w terminie uzgodnionym z Zamawiającym, nie później niż 30 dni po każdej zmianie funkcjonalności,
i. utrzymaniu i aktualizacji kodu systemu w repozytorium kodu udostępnionym przez Zamawiającego za pomocą funkcjonalności *Bitbucket* pakietu *Atlassian*, w terminie czasie uzgodnionym z Zamawiającym, nie później niż 30 dni od zgłoszenia.

j. realizacji, w zakresie uzgodnionym z Zamawiającym w ramach Analizy Przedwdrożeniowej, o której mowa w Rozdziale 8, wszelkich aktualizacji systemu z wykorzystaniem technik i narzędzi dla *Continuous Delivery/Continuous Deployment*, w czasie uzgodnionym z Zamawiającym, nie później niż 30 dni od zgłoszenia,

k. przetestowaniu z wykorzystaniem testów jednostkowych, modułowych i integracyjnych wszelkich aktualizacji przed ich zainstalowaniem na serwery produkcyjne, aby zapewnić bezawaryjne działanie Systemu,

l. okresowo, nie rzadziej niż raz na 90 dni analizę środowiska, w tym w szczególności serwerów aplikacyjnych i baz danych – analiza musi zawierać opis stanu zasobów podlegających przeglądowi oraz wnioski i szczegółowe rekomendacje obejmujące informację zawierającą rekomendowane zmiany, aktualizacje, zmiany wersji danego elementu środowiska, itp.

WUG-2. Usługa wsparcia będzie realizowana w następujących formach i trybie:

a. pomoc telefoniczna realizowana przez przeszkolonych konsultantów Wykonawcy, dostępna w dni robocze w godzinach 9:00 – 16:00,

b. pomoc realizowana za pośrednictwem systemu Jira lub poczty elektronicznej dostępnej 24 godziny na dobę; czas reakcji Wykonawcy na zgłoszenie przekazane za pośrednictwem systemu Jira lub poczty elektronicznej wyniesie nie więcej niż 3 (trzy) godzinę w przypadku zgłoszeń wpływających w dni robocze,

c. aktualizację oprogramowania systemowego będą odbywały się w czasie uzgodnionym z Zamawiającym, nie później niż 30 dni od zgłoszenia;

WUG-3. Minimalny wymagany przez Zamawiającego okres świadczenia Usługi wsparcia wynosi 12 miesięcy od dnia podpisania Protokołu Odbioru Końcowego.