

# OPIS ZAŁOŻEŃ PROJEKTU INFORMATYCZNEGO

Tytuł projektu	Rozbudowa Katalogu Usług Rządowej Chmury Obliczeniowej (Rozbudowa_RChO)		
Wnioskodawca	Minister Cyfryzacji		
Beneficjent	Ministerstwo Cyfryzacji		
Partnerzy	nie dotyczy		
Źródło finansowania	Środki UE: Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Priorytet FERC.02 Zaawansowane usługi cyfrowe, Działanie FERC.02.01 „Wysoka jakość i dostępność e-usług publicznych” Budżet państwa: część budżetowa 27 – Informatyzacja		
Całkowity koszt projektu	173 000 000,00 zł		
Planowany okres realizacji projektu	10-2025 do 10-2028		
Osoba kontaktowa	Mariusz Świerczyński	Mariusz.Swierczynski@cyfra.gov.pl	880170639

## 1. POWODY PODJĘCIA PROJEKTU

### 1.1. Identyfikacja problemu i potrzeb

W związku z rosnącym ryzykiem cyberzagrożeń oraz obowiązkiem zapewnienia ciągłości działania systemów IT administracji publicznej, zobowiązani jesteśmy do spełnienia wymagań Ustawy o Krajowym systemie cyberbezpieczeństwa (KSC), dyrektywy NIS2 oraz uchwały Rady Ministrów o Wspólnej Infrastrukturze Informatycznej Państwa (Projekt WIIP). W odpowiedzi na te wymagania realizowany będzie projekt „Rozbudowa Katalogu Usług Rządowej Chmury Obliczeniowej”, w ramach którego zostanie wytworzony zestaw usług chmurowych wspierających bezpieczeństwo, ciągłość działania, zgodność prawną i cyfryzację urzędów. Ponadto realizacja niniejszego projektu umożliwi znaczące zwiększenie potencjału aktualnie świadczonych usług chmurowych (Usługi RChO) w ramach Rządowej Chmury Obliczeniowej (RChO), a także rozwinięcie i poszerzenie oferty o nowe, zaawansowane Usługi RChO. Projekt przyczyni się do lepszego wykorzystania istniejącej infrastruktury, wdrożenia nowoczesnych technologii oraz rozszerzenia funkcjonalności systemów IT administracji rządowej, umożliwiając ich dostosowanie do dynamicznie zmieniających się trendów technologicznych. Biznesowe uzasadnienie rozbudowy RChO wynika z rosnącego zapotrzebowania na dostępne Usługi RChO oraz konieczności wdrożenia nowych komponentów chmurowych:

- 1.BaaS-Backup as a Service (usługa typu SaaS) – centralne, skalowalne i bezpieczne mechanizmy tworzenia kopii zapasowych
- 2.APIaaS-API Gateway (usługa typu PaaS) – zarządzanie i zabezpieczanie komunikacji między systemami
- 3.MONaaS-Monitoring as a Service (usługa typu SaaS) – monitorowanie zasobów i usług w czasie rzeczywistym
- 4.SOCaaS-Security Operations Center as a Service (usługa typu SaaS) – usługa reagowania na incydenty i zarządzania bezpieczeństwem
- 5.SMSaaS-usługa wysyłki wiadomości SMS (usługa typu SaaS) – komunikacja z użytkownikami końcowymi
- 6.VDaaS-Virtual Desktop as a Service (usługa typu SaaS)
- 7.VM-GPU-maszyny wirtualne z kartą GPU (usługa typu IaaS)

## 8. Usługi AI-np. RAG, itp. (usługi typu SaaS).

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
Ministerstwo Cyfryzacji	<ul style="list-style-type: none"> <li>przestarzała infrastruktura teleinformatyczna;</li> <li>systemy typu legacy, które są trudne w utrzymaniu i rozwoju;</li> <li>ograniczenia skalowalności infrastruktury IT;</li> <li>długotrwałe wdrażania nowych systemów związane z procedurami pzp;</li> <li>problemy z dostępnością systemów w okresach szczytowych (pik wydajności).</li> </ul>	1
Podmioty administracji rządowej realizujące projekty wymagające rozwoju infrastruktury IT (95 jednostek oraz 16 urzędów wojewódzkich wraz z podmiotami podległymi)	<ul style="list-style-type: none"> <li>przestarzała infrastruktura teleinformatyczna;</li> <li>systemy typu legacy, które są trudne w utrzymaniu i rozwoju;</li> <li>brak integracji pomiędzy systemami IT w różnych organizacjach;</li> <li>niewystarczające środki finansowe na utrzymanie systemów IT;</li> <li>ograniczenia skalowalności infrastruktury IT;</li> <li>długotrwałe wdrażania nowych systemów związane z procedurami pzp;</li> <li>niewystarczający poziom bezpieczeństwa infrastruktury oraz systemów transmisji i przetwarzania danych;</li> <li>problemy z dostępnością systemów w okresach szczytowych (pik wydajności);</li> <li>brak kompetencji cyfrowych kadry.</li> </ul>	111
Jednostki administracji samorządowej	<ul style="list-style-type: none"> <li>rozproszona infrastruktura IT;</li> <li>nieefektywne serwerownie, generujące wysokie koszty jednostkowe;</li> <li>przestarzałe rozwiązania informatyczne;</li> <li>niewystarczające cyberbezpieczeństwo;</li> <li>słaba współpraca z administracją rządową w obszarze IT;</li> <li>brak jednolitych rozwiązań IT;</li> <li>ograniczone finansowanie – niedofinansowanie projektów;</li> <li>niskie kompetencje cyfrowe pracowników;</li> <li>niechęć do zmian technologicznych.</li> </ul>	2807

## 1.2. Opis stanu obecnego

Minister Cyfryzacji formalnie pełniący rolę Operatora RChO zbudował i utrzymuje chmurę rządową w oparciu o własną infrastrukturę informatyczną oraz zasoby COI i NASK. W ramach projektu POPC została zbudowana inicjalna część chmury rządowej, która w ramach tej inicjatywy będzie rozbudowana. W oparciu o tę infrastrukturę dostarczane są dla instytucji rządowych wskazanych w Uchwale WIIP usługi chmurowe opisane w Katalogu Usług RChO.

Większość z tych usług to usługi infrastrukturalne typu IaaS. W oparciu o tę infrastrukturę zbudowana została inicjalna wersja usługi EZD RP dostarczana w modelu SaaS. Trwają postępowania zakupowe mające na celu rozbudowanie infrastruktury RChO aby mogła dostarczać usługę SaaS EZD RP dla co najmniej 300 000 użytkowników. W kolejnym roku planowana jest rozbudowa do obsługi 600 000 użytkowników.

Obecna infrastruktura RChO składa się z kilku kluczowych komponentów, które zapewniają zestaw usług chmurowych opisanych w Katalogu Usług RChO, wykorzystywane na potrzeby kilku Odbiorców Usług lokując na jej zasobach ponad 40 systemów informatycznych.

- Centra Danych - usługi dostępne są z dwóch lokalizacji Centrum Danych zlokalizowanych na terenie Warszawy. Oba ośrodki są aktywne i każde z nich samodzielnie dostarcza Usługi RChO;
- Dane pomiędzy lokalizacjami RChO mogą być replikowane synchronicznie;
- Usługi RChO – dostępne usługi chmurowe typu IaaS, PaaS, SaaS zgodnie z Katalogiem Usług RChO;
- Bezpieczeństwo – zabezpieczenia fizyczne i zabezpieczenia logiczne dostarczane przez RKB, SOC, NOC, SIEM;
- Zarządzanie i monitoring zasobów – systemy zarządzania i monitorowania zasobów informatycznych, ITSM, SAM, CMP.

Realizacja inwestycji zapewni możliwość obsługi dodatkowych systemów administracji rządowej, rozbudowę funkcjonalną, zapewnienie ciągłości działania, zapewnienie utrzymania w stanie zgodnym z aktualnymi standardami technologicznymi oraz ograniczania powstawania wtórnego długu technologicznego dla systemów informatycznych hostowanych w RChO.

## 2. EFEKTY PROJEKTU

### 2.1. Cele i korzyści wynikające z projektu

<b>Cel - 1</b>	Podniesienie poziomu odporności systemów informatycznych administracji publicznej oraz osiągnięcie zdolności do skutecznego reagowania na incydenty poprzez wdrożenie rozwiązań zgodnych z celem strategicznym.
<b>Cel strategiczny</b>	Strategia Cyberbezpieczeństwa RP na lata 2019-2024, Cel szczegółowy 2: Podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym wynikający z dokumentu.
<b>Korzyść:</b>	1) Zwiększenie odporności operacyjnej poprzez utrzymanie ciągłości działania systemów administracji publicznej oraz zmniejszenie podatności na incydenty ransomware i zakłócenia infrastruktury RChO; 2) Zgodność z regulacjami krajowymi i unijnymi poprzez spełnienie wymogów Ustawy o KSC, dyrektywy NIS2, RODO; 3) Centralizacja i ujednolicenie zarządzania bezpieczeństwem poprzez lepszą kontrolę, widoczność i nadzór nad systemami informatycznymi Odbiorców Usług dzięki planowanym usługom RChO (BaaS, MONaaS, SMSaaS, APIaaS); 4) Szybsze wykrywanie i neutralizacja zagrożeń dzięki skróceniu czasu reakcji na incydenty oraz udostępnienie usługi SOCaaS.
<b>KPI:</b>	KPI 1: Liczba tenantów wykorzystujących usługę BaaS i WORM; KPI 2: Liczba tenantów wykorzystujących usługę SOCaaS; KPI 3: Liczba tenantów wykorzystujących usługę MONaaS; KPI 4: Liczba przerw w świadczeniu Usług RChO z powodu cyberincydentów; KPI 5: Średni czas reakcji na incydent; KPI 6: Liczba wykrytych niezgodności w audytach bezpieczeństwa.
<b>Wartość</b>	KPI 1: Wartość aktualna: 0 szt.;

<b>aktualna i docelowa KPI:</b>	<p>KPI 2: Wartość aktualna: 0 szt.;</p> <p>KPI 3: Wartość aktualna: 0 szt.;</p> <p>KPI 4: Wartość aktualna: brak pomiarów;</p> <p>KPI 5: Wartość aktualna: 3 godziny;</p> <p>KPI 6: Wartość aktualna: brak pomiarów;</p> <p>KPI 1: Wartość docelowa: 30 szt.;</p> <p>KPI 2: Wartość docelowa: 30 szt.;</p> <p>KPI 3: Wartość docelowa: 10 szt.;</p> <p>KPI 4: Wartość docelowa: &lt; 10;</p> <p>KPI 5: Wartość docelowa: 2 godziny;</p> <p>KPI 6: Wartość docelowa: 0 krytycznych i &lt;3 niekrytycznych.</p>
<b>Metoda pomiaru KPI</b>	<p>KPI 1: Metoda pomiaru: automatycznie generowane raporty wykorzystania usług elektronicznych. Źródło pomiaru: dokumentacja zarządcza projektu. Częstotliwość pomiaru: wskaźnik będzie monitorowany w sposób ciągły (raport zbiorczy min. raz do roku). Ostateczny pomiar nastąpi w dniu zakończenia realizacji projektu. Za monitoring wskaźnika będzie odpowiedzialny zespół administratorów RChO (COI).</p> <p>KPI 2: Metoda pomiaru: automatycznie generowane raporty wykorzystania usług elektronicznych. Źródło pomiaru: dokumentacja zarządcza projektu. Częstotliwość pomiaru: wskaźnik będzie monitorowany w sposób ciągły (raport zbiorczy min. raz do roku). Ostateczny pomiar nastąpi w dniu zakończenia realizacji projektu. Za monitoring wskaźnika będzie odpowiedzialny zespół administratorów RChO (COI).</p> <p>KPI 3: Metoda pomiaru: automatycznie generowane raporty wykorzystania usług elektronicznych. Źródło pomiaru: dokumentacja zarządcza projektu. Częstotliwość pomiaru: wskaźnik będzie monitorowany w sposób ciągły (raport zbiorczy min. raz do roku). Ostateczny pomiar nastąpi w dniu zakończenia realizacji projektu. Za monitoring wskaźnika będzie odpowiedzialny zespół administratorów RChO (COI).</p> <p>KPI 4: Metoda pomiaru: automatycznie generowane raporty wykorzystania usług elektronicznych. Źródło pomiaru: dokumentacja zarządcza projektu. Częstotliwość pomiaru: wskaźnik będzie monitorowany w sposób ciągły (raport zbiorczy min. raz do roku). Ostateczny pomiar nastąpi w dniu zakończenia realizacji projektu. Za monitoring wskaźnika będzie odpowiedzialny zespół administratorów RChO (COI).</p> <p>KPI 5: Metoda pomiaru: automatycznie generowane raporty wykorzystania usług elektronicznych. Źródło pomiaru: dokumentacja zarządcza projektu. Częstotliwość pomiaru: wskaźnik będzie monitorowany w sposób ciągły (raport zbiorczy min. raz do roku). Ostateczny pomiar nastąpi w dniu zakończenia realizacji projektu. Za monitoring wskaźnika będzie odpowiedzialny zespół administratorów RChO (COI).</p> <p>KPI 6: Metoda pomiaru: automatycznie generowane raporty wykorzystania usług elektronicznych. Źródło pomiaru: dokumentacja zarządcza projektu. Częstotliwość pomiaru: wskaźnik będzie monitorowany w sposób ciągły (raport zbiorczy min. raz do roku). Ostateczny pomiar nastąpi w dniu zakończenia realizacji projektu. Za monitoring wskaźnika będzie odpowiedzialny zespół administratorów RChO (COI).</p>

<b>Cel - 2</b>	Cyfryzacja usług publicznych, Cel:100 % kluczowych usług publicznych jest dostępnych online dla obywateli i przedsiębiorstw w Unii i, w stosownych przypadkach, istnieje możliwość interakcji online z administracją publiczną (decyzja nr 2022/2481 pkt 4).
<b>Cel strategiczny</b>	„Droga ku cyfrowej dekadzie” do 2030 r. (Digital Europe 2030): Cel cyfrowy 4 Cyfryzacja usług publicznych, Cel G.
<b>Korzyść:</b>	1) Szersze wykorzystanie technologii cyfrowych w administracji publicznej i gospodarce; 2) Przyspieszenie transformacji cyfrowej; 3) Rozwój cyfrowych usług publicznych, które będą dostępne dla obywateli i przedsiębiorców w jeszcze większym zakresie.
<b>KPI:</b>	KPI 1: Liczba tenantów wykorzystujących usługę maszyna wirtualna z GPU; KPI 2: Liczba tenantów wykorzystujących usługę API Gateway; KPI 3: Liczba tenantów wykorzystujących usługę VDaaS; KPI 4: Liczba tenantów wykorzystujących usługę SMSaaS; KPI 5: Liczba systemów informatycznych wykorzystujących modele AI dostarczane jako usługa RChO; KPI 6: Średni poziom dostępności świadczonych usług (SLA).
<b>Wartość aktualna i docelowa KPI:</b>	KPI 1: Wartość aktualna: 0 szt.; KPI 2: Wartość aktualna: 0 szt.; KPI 3: Wartość aktualna: 0 szt.; KPI 4: Wartość aktualna: 0 szt.; KPI 5: Wartość aktualna: 0 szt.; KPI 6: Wartość aktualna: 98,75%. KPI 1: Wartość docelowa: 5 szt.; KPI 2: Wartość docelowa: 3 szt.; KPI 3: Wartość docelowa: 5 szt.; KPI 4: Wartość docelowa: 3 szt.; KPI 5: Wartość docelowa: 3 szt.; KPI 6: Wartość docelowa: 99,5%.
<b>Metoda pomiaru KPI</b>	KPI 1: Metoda pomiaru: automatycznie generowane raporty wykorzystania usług elektronicznych. Źródło pomiaru: dokumentacja zarządcza projektu. Częstotliwość pomiaru: wskaźnik będzie monitorowany w sposób ciągły (raport zbiorczy min. raz do roku). Ostateczny pomiar nastąpi w dniu zakończenia realizacji projektu. Za monitoring wskaźnika będzie odpowiedzialny zespół administratorów RChO (COI). KPI 2: Metoda pomiaru: automatycznie generowane raporty wykorzystania usług elektronicznych. Źródło pomiaru: dokumentacja zarządcza projektu. Częstotliwość pomiaru: wskaźnik będzie monitorowany w sposób ciągły (raport zbiorczy min. raz do roku). Ostateczny pomiar nastąpi w dniu zakończenia realizacji projektu. Za monitoring wskaźnika będzie odpowiedzialny zespół administratorów RChO (COI). KPI 3: Metoda pomiaru: automatycznie generowane raporty wykorzystania usług elektronicznych. Źródło pomiaru: dokumentacja zarządcza projektu. Częstotliwość pomiaru: wskaźnik będzie monitorowany w sposób ciągły (raport zbiorczy min. raz do roku). Ostateczny pomiar nastąpi w dniu zakończenia realizacji projektu. Za monitoring wskaźnika będzie odpowiedzialny zespół administratorów RChO (COI).

	<p>KPI 4: Metoda pomiaru: automatycznie generowane raporty wykorzystania usług elektronicznych. Źródło pomiaru: dokumentacja zarządcza projektu. Częstotliwość pomiaru: wskaźnik będzie monitorowany w sposób ciągły (raport zbiorczy min. raz do roku). Ostateczny pomiar nastąpi w dniu zakończenia realizacji projektu. Za monitoring wskaźnika będzie odpowiedzialny zespół administratorów RChO (COI).</p> <p>KPI 5: Metoda pomiaru: automatycznie generowane raporty wykorzystania usług elektronicznych. Źródło pomiaru: dokumentacja zarządcza projektu. Częstotliwość pomiaru: wskaźnik będzie monitorowany w sposób ciągły (raport zbiorczy min. raz do roku). Ostateczny pomiar nastąpi w dniu zakończenia realizacji projektu. Za monitoring wskaźnika będzie odpowiedzialny zespół administratorów RChO (COI).</p> <p>KPI 6: Metoda pomiaru: automatycznie generowane raporty wykorzystania usług elektronicznych. Źródło pomiaru: dokumentacja zarządcza projektu. Częstotliwość pomiaru: wskaźnik będzie monitorowany w sposób ciągły (raport zbiorczy min. raz do roku). Ostateczny pomiar nastąpi w dniu zakończenia realizacji projektu. Za monitoring wskaźnika będzie odpowiedzialny zespół administratorów RChO (COI).</p>
<b>Cel - 3</b>	Zapewnienie wysokiego poziomu usług świadczonych społeczeństwu przez administrację publiczną.
<b>Cel strategiczny</b>	„Droga ku cyfrowej dekadzie” do 2030 r. oraz Krajowy plan działania do programu polityki „Droga ku cyfrowej dekadzie” do 2030 r. Projekt wpisuje się w cel ogólny – G. „Zapewnienie inkluzywnych, cyfrowych usług publicznych” Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Działanie FERC.02.01 Wysoka jakość i dostępność e-usług publicznych.
<b>Korzyść:</b>	Dedykowany katalog usług dla administracji rządowej przyczyni się do poprawy jakości obsługi użytkowników końcowych oraz zwiększenia efektywności finansowej realizacji zadań publicznych w zakresie technologii informatycznych.
<b>KPI:</b>	<p>KPI 1: Liczba jednostek administracji rządowej korzystających z Usług RChO;</p> <p>KPI 2: Liczba wystąpień usług wewnątrzadministracyjnych (A2A);</p> <p>KPI 3: Liczba uruchomionych systemów teleinformatycznych w podmiotach wykonujących zadania publiczne;</p> <p>KPI 4: Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych;</p> <p>KPI 5: Instytucje publiczne otrzymujące wsparcie na opracowywanie usług, produktów i procesów cyfrowych.</p>
<b>Wartość aktualna i docelowa KPI:</b>	<p>KPI 1: Wartość aktualna: 6 szt.;</p> <p>KPI 2: Wartość aktualna: 14 szt.;</p> <p>KPI 3: Wartość aktualna: 45 szt.;</p> <p>KPI 4: Wartość aktualna: 6;</p> <p>KPI 5: Wartość aktualna: 0.</p> <p>KPI 1: Wartość docelowa: 15 szt.;</p> <p>KPI 2: Wartość docelowa: 24 szt.;</p> <p>KPI 3: Wartość docelowa: 90 szt.;</p> <p>KPI 4: Wartość docelowa: 15;</p> <p>KPI 5: Wartość docelowa: 1.</p>
<b>Metoda</b>	KPI 1:

pomiaru KPI	<p>Metoda pomiaru: automatycznie generowane raporty wykorzystania usług elektronicznych. Źródło pomiaru: dokumentacja zarządcza projektu. Częstotliwość pomiaru: wskaźnik będzie monitorowany w sposób ciągły (raport zbiorczy min. raz do roku). Ostateczny pomiar nastąpi w dniu zakończenia realizacji projektu. Za monitoring wskaźnika będzie odpowiedzialny zespół administratorów RChO (COI).</p> <p>KPI 2:</p> <p>Metoda pomiaru: automatycznie generowane raporty wykorzystania usług elektronicznych. Źródło pomiaru: dokumentacja zarządcza projektu. Częstotliwość pomiaru: wskaźnik będzie monitorowany w sposób ciągły (raport zbiorczy min. raz do roku). Ostateczny pomiar nastąpi w dniu zakończenia realizacji projektu. Za monitoring wskaźnika będzie odpowiedzialny zespół administratorów RChO (COI).</p> <p>KPI 3:</p> <p>Metoda pomiaru: automatycznie generowane raporty wykorzystania usług elektronicznych. Źródło pomiaru: dokumentacja zarządcza projektu. Częstotliwość pomiaru: wskaźnik będzie monitorowany w sposób ciągły (raport zbiorczy min. raz do roku). Ostateczny pomiar nastąpi w dniu zakończenia realizacji projektu. Za monitoring wskaźnika będzie odpowiedzialny zespół administratorów RChO (COI).</p> <p>KPI 4:</p> <p>Metoda pomiaru: automatycznie generowane raporty wykorzystania usług elektronicznych. Źródło pomiaru: dokumentacja zarządcza projektu. Częstotliwość pomiaru: wskaźnik będzie monitorowany w sposób ciągły (raport zbiorczy min. raz do roku). Ostateczny pomiar nastąpi w dniu zakończenia realizacji projektu. Za monitoring wskaźnika będzie odpowiedzialny zespół administratorów RChO (COI).</p> <p>KPI 5:</p> <p>Metoda pomiaru: automatycznie generowane raporty wykorzystania usług elektronicznych. Źródło pomiaru: dokumentacja zarządcza projektu. Częstotliwość pomiaru: wskaźnik będzie monitorowany w sposób ciągły (raport zbiorczy min. raz do roku). Ostateczny pomiar nastąpi w dniu zakończenia realizacji projektu. Za monitoring wskaźnika będzie odpowiedzialny zespół administratorów RChO (COI).</p>
-------------	--

## 2.2. Udostępnione e-usługi

Lp.	Nazwa e-usługi	Typ	Zakres oddziaływania	Poziom dojrzałości e-usługi
1	Usługa w zakresie infrastruktury IT (IaaS) oraz platform systemowych	A2A	Ministerstwo Cyfryzacji Podmioty administracji rządowej realizujące projekty wymagające rozwoju infrastruktury IT (95 jednostek oraz 16 urzędów wojewódzkich wraz z podmiotami podległymi) Jednostki administracji samorządowej	Nie dotyczy

Lp.	Nazwa e-usługi	Typ	Zakres oddziaływania	Poziom dojrzałości e-usługi
			(rocznie ok 12000 transakcji)	
2	Usługa w modelu chmury obliczeniowej (PaaS/SaaS)	A2A	Ministerstwo Cyfryzacji Podmioty administracji rządowej realizujące projekty wymagające rozwoju infrastruktury IT (95 jednostek oraz 16 urzędów wojewódzkich wraz z podmiotami podległymi) Jednostki administracji samorządowej (rocznie ok 12000 transakcji)	Nie dotyczy

## 2.3. Udostępnione informacje sektora publicznego i zdigitalizowane zasoby

Nie dotyczy

## 2.4. Produkty końcowe projektu

Nazwa produktu	Planowana data wdrożenia
Pozytywny raport z testów wydajności usługi „API Gateway” dostarczającej centralną bramę do zarządzania dostępem do usług i systemów IT.	11-2027
Pozytywny raport z testów wydajności usługi maszyny wirtualnej wyposażonej w kartę GPU „VM-GPU”.	12-2027
Pozytywny raport z testów wydajności usługi monitoringu „MONaaS”.	12-2027
Pozytywny raport z testów wydajności usługi tworzenia kopii bezpieczeństwa danych „BaaS” z zaimplementowanym mechanizmem WORM (Write Once Read Many).	01-2028
Pozytywny raport z testów wydajności usługi: Security Operations Center „SOCaaS” i wysłania krótkich wiadomości tekstowych SMS „SMSaaS”.	05-2028
Pozytywny raport z testów wydajności usługi wirtualnego desktopu „VDaaS”.	06-2028
Pozytywny raport z testów wydajności usług z wykorzystaniem modeli sztucznej inteligencji (AI) „MaaS”.	08-2028
Pozytywny raport z testów bezpieczeństwa RChO po rozbudowie.	09-2028
Materiały informacyjno-promocyjne	09-2028
Modyfikacja RChO	10-2028
Infrastruktura związana z rozbudową RChO (serwery z procesorami w	10-2028



Nazwa produktu	Planowana data wdrożenia
architekturze x64 oraz kartami GPU, infrastruktura LAN, przestrzeń dyskowa, oprogramowanie systemowe i narzędziowe, licencje dostępne).	

3. KAMIENIE MIŁOWE

Kamienie milowe	Planowany termin osiągnięcia
Opracowana architektura techniczna	2026-03-31
Opracowana dokumentacja przetargowa	2026-05-31
Ogłoszone postępowania przetargowe na główne elementy planowanych produktów	2026-08-31
Zakończony proces oceny ofert Wykonawców	2026-12-31
Zakończony proces dostaw sprzętu i oprogramowania	2027-05-31
Zakończony proces zakupowy	2027-07-31
Uruchomione produkcyjne usługi RChO: MONaaS, API Gateway, SMSaaS, VM-GPU	2027-12-31
Uruchomione produkcyjne usługi RChO: BaaS	2028-02-29
Uruchomione produkcyjne pozostałych usług RChO	2028-08-31
Udostępnione nowe Usługi RChO Odbiorcom Usług	2028-10-31

4. KOSZTY

4.1. Koszty ogólne projektu wraz ze sposobem finansowania

<b>Całkowity koszt projektu (netto oraz brutto), w tym</b>	Netto 141 662 807,57 zł Brutto 173 000 000,00 zł	
<b>Procent dofinansowania ze środków UE (brutto)</b>	79,71%	
<b>Procent środków z budżetu państwa (brutto)</b>	20,29%	
<b>Podział całkowitego kosztu projektu na poszczególne lata (netto oraz brutto)</b>	2025	Netto 108 327,06 zł Brutto 108 327,06 zł
	2026	Netto 24 731 857,73 zł Brutto 29 981 605,65 zł
	2027	Netto 111 332 620,00 zł Brutto 136 477 298,55 zł
	2028	Netto 5 490 002,78 zł Brutto 6 432 768,74 zł

## 4.2. Wykaz poszczególnych pozycji kosztowych

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
Oprogramowanie	Zakup oprogramowania podstawowego, zakup gotowych rozwiązań.	75 743 904,69 zł	Koszty dostaw oprogramowania oraz prac konfiguracyjno-wdrożeniowych związanych z zapewnieniem zasobów.
Infrastruktura	Niezbędne wyposażenie CPD, RACK, serwery, GPU, przestrzeń dyskowa, LAN, biblioteki taśmowe, firewall, loadbalancer.	88 541 950,48 zł	Koszty dostaw infrastruktury niezbędnej do działania usług RChO.
Koszty UX i grafiki			
Bezpieczeństwo	Przygotowanie wymagań bezpieczeństwa oraz dokumentacji zabezpieczeń systemu; Przeprowadzenie testów bezpieczeństwa.	200 000,00 zł	Koszty usług zewnętrznych związanych z zapewnieniem bezpieczeństwa, zewnętrzne audyty bezpieczeństwa i wewnętrzne testy bezpieczeństwa systemu.
Wydajność rozwiązań	Testy wydajności i stabilności -	600 000,00 zł	Wewnętrzne oraz zewnętrzne testy wydajnościowe oraz

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
	Raporty z testów wydajności.		monitorowanie i badanie wydajności systemów.
Szkolenia			
Działania informacyjno-promocyjne	Promocja projektu, materiały informacyjno-promocyjne.	2 500 000,00 zł	W ramach tej kategorii przewidziano koszty obligatoryjnych działań informacyjnych właściwych dla FERC oraz działań promocyjnych adresowanych do podmiotów administracji rządowej, mających na celu jak najszersze wykorzystanie zakresu udostępnianych usług.
Koszty zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego)	Koszty zatrudnienia kierownika projektu i personelu wspomagającego.	5 414 144,83 zł	Na etapie prac przygotowawczych koszty zespołu zarządzającego zostały oszacowane na podstawie skali i specyfiki planowanych działań, określenia ról projektowych niezbędnych do prawidłowej realizacji projektu oraz zapewnienia prawidłowego nadzoru i współpracy z wykonawcami.

#### 4.3. Koszty ogólne utrzymania wraz ze sposobem finansowania (okres 5 lat)

Całkowity koszt utrzymania trwałości projektu (brutto)	188 142 402,85 zł		Źródło finansowania
Podział całkowitego kosztu utrzymania trwałości projektu na poszczególne lata (netto oraz brutto)	2028	535 433,67 zł (brutto) (435 311,93 zł netto)	krajowe środki publiczne - budżet państwa
	2029	2 677 168,37 zł (brutto) (2 176 559,65 zł netto)	krajowe środki publiczne - budżet państwa
	2030	2 837 798,48 zł (brutto) (2 307 153,24 zł netto)	krajowe środki publiczne - budżet państwa
	2031	33 586 100,50 zł (brutto) (27 305 772,76 zł netto)	krajowe środki publiczne - budżet państwa
	2032	148 505 901,83 zł (brutto)	krajowe środki

		(120 736 505,55 zł netto)	publiczne - budżet państwa
--	--	---------------------------	----------------------------

#### 4.4. Planowane koszty ogólne realizacji (w przypadku projektu współfinansowanego – wkład krajowy z budżetu państwa) oraz koszty utrzymania projektu:

- zostaną pokryte w ramach budżetów odpowiednich dysponentów części budżetowych bez konieczności występowania o dodatkowe środki z budżetu państwa
- ~~- będą powodować konieczność przyznania dodatkowych kwot~~

## 5. GŁÓWNE RYZYKA

### 5.1. Ryzyka wpływające na realizację projektu

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Zbyt mały lub zbyt duży popyt na usługi oferowane przez RChO	Średnia	Średnie	Podjęcie działań promocyjnych i regulacyjnych (pobudzanie popytu) oraz zapewnienie skalowalności infrastruktury w celu dostosowania do popytu.
Nadmierny popyt na usługi oferowane w wyniku realizacji projektu	Mała	Wysokie	Planowanie dalszego rozwoju potencjału RChO.
Niezakończenie postępowań zakupowych w terminach zgodnych z założeniami harmonogramu	Duża	Wysokie	Zastosowanie dwustopniowej procedury wyboru wykonawców. Przyspieszenie terminu publikacji ogłoszenia.
Brak wystarczających zasobów kadrowych o odpowiednich kwalifikacjach dotyczących zagadnień związanych ze sztuczną inteligencją (AI)	Duża	Wysokie	Zapewnienie wsparcia szkoleniowego oraz odpowiedniego funduszu wynagrodzeń.

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Brak wystarczających zasobów kadrowych	Duża	Wysokie	Zapewnienie wsparcia szkoleniowego oraz odpowiedniego funduszu wynagrodzeń.
Nieosiągnięcie wskaźników produktu oraz celu projektu	Średnia	Średnie	Zapewnienie monitoringu projektu.

## 5.2. Ryzyka wpływające na utrzymanie efektów

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Niski popyt na usługi oferowane w wyniku realizacji projektu – brak wykorzystania pełnego potencjału środowiska obliczeniowego i usług chmurowych przez użytkowników końcowych.	Duża	Średnie	Podjęcie działań promocyjnych i regulacyjnych (pobudzanie popytu).
Brak możliwości zatrudnienia osób o odpowiednich kompetencjach niezbędnych do utrzymania efektów projektu.	Średnia	Średnie	Powołanie zespołów dedykowanych wyłącznie dla tego projektu (nierealizujących prac w innych projektach).
Brak wystarczających środków finansowych na zapewnienie długoterminowego utrzymania i funkcjonowania efektów projektu	Średnia	Średnie	Wczesne zaangażowanie działów operacyjnych; Zabezpieczenie budżetu operacyjnego; Model finansowania zagwarantowany ustawowo.

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Nieosiągnięcie wszystkich zaplanowanych korzyści	Duża	Średnie	Wczesne zaangażowanie interesariuszy; Zarządzanie zmianą – komunikacja, szkolenia, wsparcie użytkowników; Walidacja korzyści – testy; Monitorowanie KPI po ich wdrożeniu.

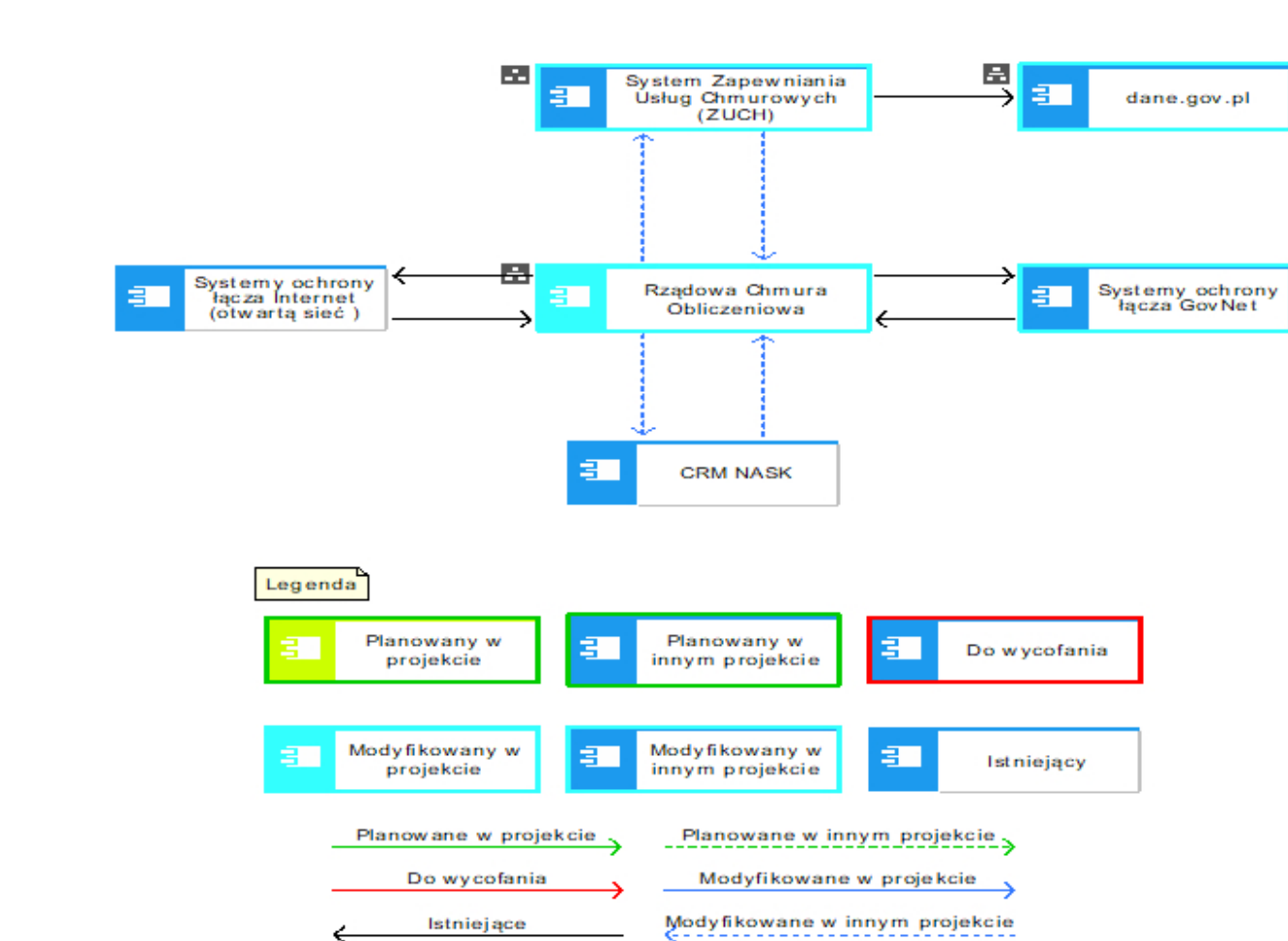
## 6. OTOCZENIE PRAWNE

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
1	Uchwała Rady Ministrów w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa”.	TAK/NIE		
2	Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne.	TAK/NIE		
3	Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.	TAK/NIE		
4	Ustawa o krajowym systemie cyberbezpieczeństwa.	TAK/NIE		
5	Ustawa o ochronie baz danych.	TAK/NIE		
6	Ustawa o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego.	TAK/NIE		
7	Ustawa o wspieraniu rozwoju usług i sieci telekomunikacyjnych.	TAK/NIE		
8	Rozporządzenie Ministra Cyfryzacji w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników.	TAK/NIE		
9	Rozporządzenie Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego.	TAK/NIE		
10	Ustawa o narodowym zasobie archiwalnym i archiwach.	TAK/NIE		

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
11	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148, Dyrektywa NIS2	TAK/NIE		

## 7. ARCHITEKTURA

### 7.1. Widok kooperacji aplikacji



### Lista systemów wykorzystywanych w projekcie

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
1	CRM NASK	Naukowa i Akademicka Sieć Komputerowa	<p>CRM NASK to system zbudowany w oparciu o oprogramowanie EspoCRM wraz z rozszerzeniami Advanced Pack, Sales Pack, Outlook Integration, VoIP Integration oraz innymi modyfikacjami wykonanymi na zlecenie NASK PIB. System został wdrożony w NASK PIB w celu usprawnienia procesu wdrażania EZD RP (EZD PUW) oraz obsługi użytkowników EZD RP (EZD PUW). W systemie są gromadzone m.in. informacje o organizacjach, kontaktach, umowach, szkoleniach, wdrożeniach, zgłoszeniach, dostępach realizowanych na rzecz podmiotów wdrażających EZD RP (EZD PUW).</p> <p>Najważniejsze moduły: a. Poczta – umożliwia gromadzenie i obsługę korespondencji e-mailowej; b. Rozmowy – umożliwia gromadzenie informacji o rozmowach telefonicznych z klientami; c. Zadania – umożliwia realizację wewnętrznych zadań użytkowników; d. Kalendarz – umożliwia planowania spotkań (w tym szkoleń); e. Marketing – umożliwia tworzenie list dystrybucyjnych i masową wysyłkę wiadomości przez maile transakcyjne; f. Zainteresowani – umożliwia gromadzenie informacji o jednostkach</p>	Istniejący	Brak zmian



Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			<p>zainteresowanych wdrożeniem EZD RP; g. Kontakty–umożliwia gromadzenie informacji o osobach w tym uprawnieniu do obsługi zgłoszeń serwisowych; h. Szanse–umożliwia m.in. obsługę procesu przedwdrożeniowego (analizę możliwości wdrożenia) w podmiocie; i. Organizacje–umożliwia gromadzenie informacji o podmiotach w tym ich klasyfikacji; j. Umowy–umożliwia gromadzenie informacji i dokumentów formalnych; k. Wdrożenia–służy do gromadzenia informacji związanych z przebiegiem wdrożenia; l. Szkolenia–służy do gromadzenia informacji o zrealizowanych szkoleniach w podmiocie; m. Zgłoszenia–obsługa zgłoszeń serwisowych; n. Adresy IP–umożliwia gromadzenie informacji o adresach IP i nadanych dla nich dostępach; o. Baza wiedzy; p. Raporty–tworzenie różnych raportów; q. Portal partnera–umożliwia dostęp kontaktów do danych zapisanych w systemie.</p> <p>Istniejące integracje: REGON(GUS); TERYT(GUS); EZD PUW; JIRA; OFFICE365; Active Directrory; Authentik; GetResponse; Webankieta; ITSM.</p>		
2	dane.gov.pl	Ministerstwo	Dane.gov.pl (portal danych) to prowadzony	Modyfikowany	Brak zmian

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
		Cyfryzacji	przez ministra właściwego do spraw informatyzacji, powszechnie dostępny system teleinformatyczny, służący do udostępniania informacji sektora publicznego w celu ponownego wykorzystywania. Portal funkcjonuje na podstawie ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz.U. z 2023 r. poz. 1524) oraz rozporządzenia Rady Ministrów z dnia 21 listopada 2022 r. w sprawie portalu danych (Dz.U. z 2022 r. poz. 2415).		
3	Rządowa Chmura Obliczeniowa	Ministerstwo Cyfryzacji	Rządowa Chmura Obliczeniowa (RChO) to system informatyczny utworzony w celu dostarczania infrastruktury informatycznej dla podmiotów administracji publicznej w modelu chmury obliczeniowej. RChO nie prowadzi rejestrów ale może udostępniać swoje zasoby dla prowadzenia rejestrów przez uprawnione organizacje (gestora systemu), który we własnym zakresie nim zarządza i administruje. RChO integruje się z systemem: a. ZUCH w obszarze obsługi zgłoszeń oraz incydentów, raportowania oraz monitorowania	Modyfikowany	Zwiększenie potencjału wytwórczego, dodanie niezbędnego wyposażenia CPD, RACK, serwery, GPU, przestrzeń dyskowa, LAN, biblioteki taśmowe, firewall, loadbalancer. Zakup oprogramowania podstawowego oraz gotowych rozwiązań.

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			<p>wykorzystania usług RChO przez gestorów systemów w hostowanych RChO;</p> <p>b. CRM NASK w obszarze obsługi użytkowników usługi SaaS EZD RP hostowanej w RChO.</p> <p>c. RChO to chmura wspólnotowa administracji publicznej dostarczająca usługi chmurowe typu IaaS (np: maszyny wirtualne, dysk blokowy), PaaS oraz SaaS.</p> <p>Najważniejsze grupy funkcjonalne Rządowej Chmury Obliczeniowej to:</p> <p>a. systemy zarządzania infrastrukturą (serwery obliczeniowe i urządzenia składowania danych, komponenty LAN, oprogramowanie narzędziowe) i monitorowania zasobów, środowiska wirtualizacji, system orkiestracji usług RChO, kolekcjonowania logów oraz zarządzania usługami RChO;</p> <p>b. Katalog Usług RChO zawierający predefiniowane konfiguracje usług chmurowych (usługi RChO) opisane określonymi parametrami technicznymi, o określonej dostępności (SLA) oraz koszcie wykorzystania w okresie rozliczenia usługi RChO. Zarządzanie usługami RChO odbywa się z poziomu CMP (Cloud Management Platform);</p> <p>c. Rządowy Klaster Bezpieczeństwa (RKB) to</p>		

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			system zabezpieczania infrastruktury RChO oraz usług RChO, na który składają się rozwiązania klasy SIEM, usługi bezpieczeństwa, środki techniczne stosowane do zabezpieczenia oraz zespoły SOC i NOC.		
4	Systemy ochrony łącza GovNet	Ministerstwo Spraw Wewnętrznych i Administracji	Systemy ochrony łącza GovNet pozwalające systemom IT działającym w RChO bezpiecznie łączyć się z innymi środowiskami informatycznymi poprzez wydzieloną sieć (GovNet) zarządzaną przez MSWiA. Na system składają się zabezpieczenia RKB (np: firewall, rozwiązania SIEM) oraz zabezpieczenia po stronie sieci GovNet. Komunikacja w sieci odbywa się poprzez dedykowany system i szyfrowane kanały komunikacji, składający się z węzłów sieci GovNet na terenie całej Polski. W ramach GovNet udostępniane są kluczowe usługi takie jak: SRP (system Rejestrów Państwowych), CEPiK, wideokonferencje, telefonia tradycyjna i VoIP na rzecz administracji rządowej.	Modyfikowany	Brak zmian
5	Systemy ochrony łącza Internet (otwartą sieć)	Ministerstwo Cyfryzacji	Systemy ochrony łącza Internet pozwalające systemom informatycznym działającym w RChO bezpiecznie łączyć się z innymi systemami i środowiskami informatycznymi poprzez	Istniejący	Brak zmian

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			ogólnoświatową sieć komputerową – globalny, zdecentralizowany system powiązanych sieci komputerowych. Na system składają się zabezpieczenia dostarczane przez dostawców zewnętrznych np.: ochrona antyDDoS oraz zabezpieczenia po stronie RKB.		
6	System Zapewniania Usług Chmurowych (ZUCH)	Ministerstwo Cyfryzacji	System Zapewniania Usług Chmurowych (ZUCH) to narzędzie informatyczne służące do wsparcia administracji publicznej w procesie zamawiania usług chmur obliczeniowych oraz wsparcia w zakresie obsługi pozyskanych usług z Publicznych Chmur Obliczeniowych (PChO) oraz Rządowej Chmury Obliczeniowej (RChO). ZUCH został uruchomiony w kwietniu 2020 r. przez Ministerstwo Cyfryzacji pod adresem <a href="https://chmura.gov.pl/">https://chmura.gov.pl/</a> i jest kluczowym elementem Wspólnej Infrastruktury Informatycznej Państwa WIIP. System ZUCH umożliwia pozyskanie usług chmurowych dla Odbiorców usług poprzez udostępnione Katalogi usług RChO lub PChO. Wybór odpowiedniego katalogu usług wspiera proces kwalifikacji systemu informatycznego opisany zgodnie ze Standardami Cyberbezpieczeństwa Chmur Obliczeniowych	Modyfikowany	Brak zmian

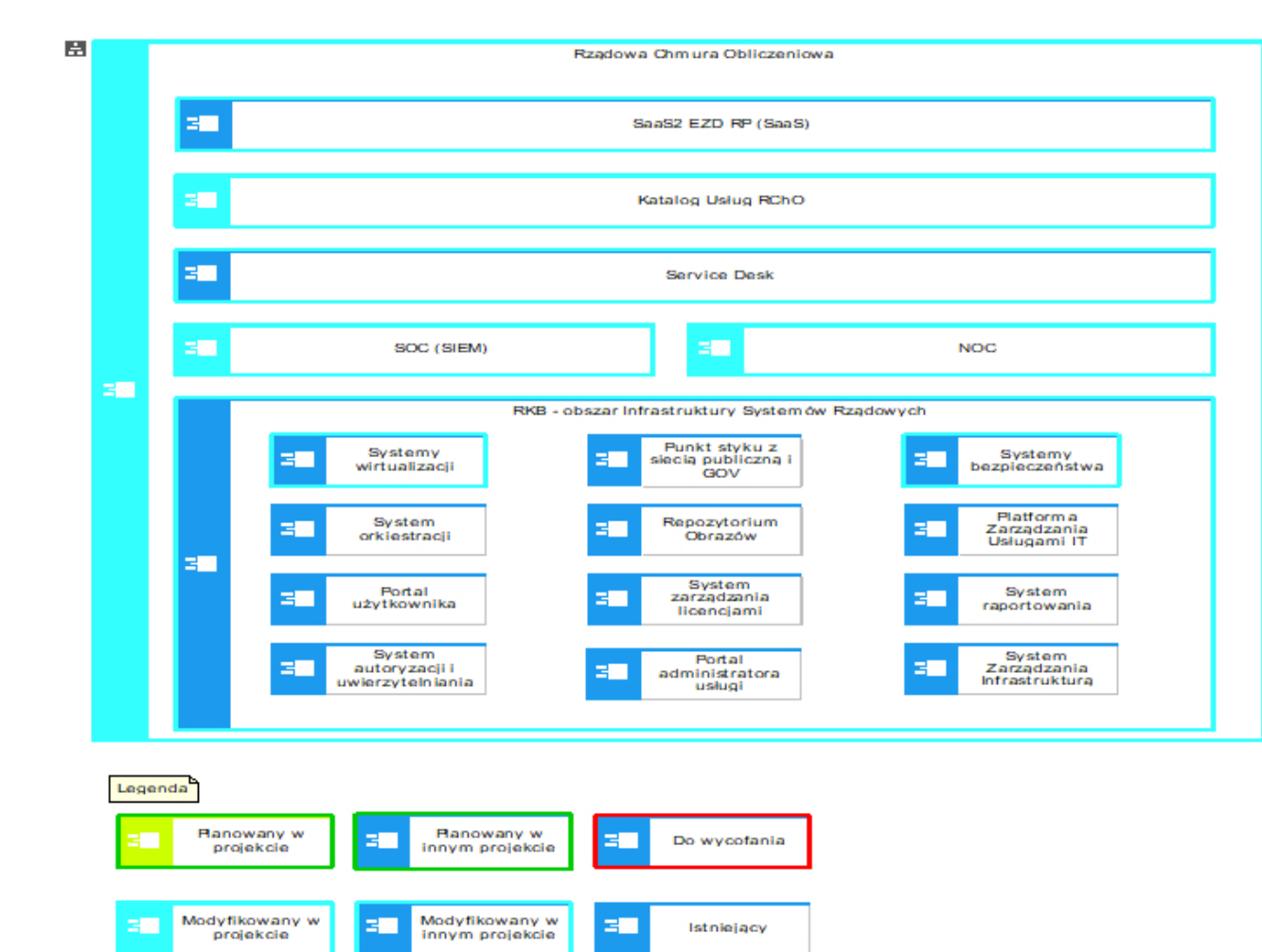
Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			(SCCO) i udostępniony w postaci ankiety na ZUCH.		

## Lista przepływów

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
1	Rządowa Chmura Obliczeniowa	CRM NASK	Dane i statusy wniosku o usługę oraz zgłoszenia incydentu.	Kopiowanie danych	realizowalny inną metodą	REST API, WhiteList
2	CRM NASK	Rządowa Chmura Obliczeniowa	Dane dotyczące zgłoszenia incydentu oraz wniosku o usługę.	Kopiowanie danych	realizowalny inną metodą	REST API
3	System Zapewniania Usług Chmurowych (ZUCH)	dane.gov.pl	Dane raportowe dotyczące użycia usług RChO, PChO	Kopiowanie danych	realizowalny inną metodą	REST API
4	Rządowa Chmura Obliczeniowa	Systemy ochrony łącza Internet (otwartą sieć)	Dane z systemów IT gestorów systemów hostowanych na RChO przesyłane do innych systemów IT poprzez publiczną sieć Internet.	Tryb odwołań bezpośrednich	krytyczny dla sukcesu projektu	REST API, S3 API, SSH/SCP/SFTP, WebSocket, VPN/IPSec, HTTPS, GUI
5	Systemy ochrony łącza Internet (otwartą sieć)	Rządowa Chmura Obliczeniowa	Dane, które nie zostały zablokowane przez systemy bezpieczeństwa np.: antyDDoS	Tryb odwołań bezpośrednich	krytyczny dla sukcesu projektu	REST API, S3 API, SSH/SCP/SFTP, WebSocket, VPN/IPSec, HTTPS
6	Systemy ochrony	Rządowa Chmura	Dane, które nie zostały	Tryb odwołań bezpośrednich	krytyczny dla sukcesu	REST API, S3 API, SSH/

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
	łącza GovNet	Obliczenia	zablokowane przez systemy bezpieczeństwa.		projektu	SCP/SFTP, WebSocket, VPN/IPSec, HTTPS, GUI
7	System Zapewniania Usług Chmurowych (ZUCH)	Rządowa Chmura Obliczeniowa	Zgłoszenie o realizację tenanta z wymaganymi zasobami i zestawem usług.	Tryb odwołań bezpośrednich	realizowalny inną metodą	REST API
8	Rządowa Chmura Obliczeniowa	Systemy ochrony łącza GovNet	Dane z systemów IT gestorów systemów hostowanych na RChO przesyłane do innych systemów IT poprzez sieć GovNet.	Tryb odwołań bezpośrednich	krytyczny dla sukcesu projektu	REST API, S3 API, SSH/SCP/SFTP, WebSocket, VPN/IPSec, HTTPS, GUI
9	Rządowa Chmura Obliczeniowa	System Zapewniania Usług Chmurowych (ZUCH)	Dane raportowe dot. użycia, kosztów, SLA:	Tryb odwołań bezpośrednich	realizowalny inną metodą	REST API

## 7.2. Kluczowe komponenty architektury rozwiązania



### 7.3. Przyjęte założenia technologiczne

Lp.	Obszar	Założenie technologiczne
1.	Infrastruktura	OpenStack, RHOV, KVM, Microsoft Hyper-V, vMware ESX, Kubernetes, mikroserwisy, containerd, rancher, kubectl, helm, Software Defined Network , Software Defined Storage
2.	Sieć i bezpieczeństwo	Firewall UTM, F5, WAF, LB, HAproxy, AntyDDoS, GovNet
3.	Standardy wymiany danych	API REST, S3 API, SSH/SCP/SFTP, WebSocket, VPN/IPSec, HTTPS, GUI
4.	Systemy operacyjne serwerowe	RedHat Enterprise Linux, Microsoft Windows Server
5.	Bazy danych	Microsoft SQL Server; PostgreSQL
6.	Serwery aplikacji	
7.	Portale	CMP (Cloud Management Portal) - portal użytkownika do zarządzania własną przestrzenią w chmurze
8.	Inne	System ZUCH

### 7.4. Opis zasobów danych przetwarzanych w planowanym



## rozwiązaniu

Czy nowy system będzie tworzył zasoby danych o charakterze rejestru publicznego?

TAK/NIE

Czy nowy system będzie przetwarzał (używał, zmieniał) zawartość innych rejestrów publicznych?

TAK/NIE

## 7.5. Bezpieczeństwo

Planowany poziom zapewnienia bezpieczeństwa (w rozumieniu przepisów §20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności [...]) (Dz. U. 2012, poz. 526 z późn. zm.) w zakresie dot. systemu zarządzania bezpieczeństwem informacji:

- ~~- system nie podlega rygorom KRI – należy wyjaśnić czy istnieją inne normy bezpieczeństwa, które będą spełnione przez system zgodnie z wymogami KRI~~
- dodatkowe zabezpieczenia powyżej wymogów KRI: należy wskazać uzasadnienie

Przedmiotem projektu jest zapewnienie odpowiednich warunków technicznych, koniecznych do udostępnienia administracji rządowej bezpiecznego i wydajnego środowiska informatycznego działającego w technologii chmury obliczeniowej. Centralnym elementem tego zamierzenia jest wdrożenie rozbudowa istniejącej Rządowej Chmury Obliczeniowej zgodnie z opracowanymi standardami bezpieczeństwa składowania i przetwarzania danych oraz sieci administracji rządowej.

Realizacja projektu zakłada rozbudowę istniejącej infrastruktury RChO (centra danych, serwery, przestrzeń dyskowa, sieci, oprogramowanie, systemy monitorowania, zespoły SOC, NOC itd.) będące w dyspozycji administracji rządowej o dodatkowe elementy infrastruktury informatycznej w następujących wątkach realizacji:

1. Rządowy Klaster Bezpieczeństwa (RKB);
2. Infrastruktura Systemów Rządowych (ISR).

Wątek RKB to opracowane i obowiązujące standardy bezpieczeństwa dla poszczególnych obszarów oraz świadczenie usług bezpieczeństwa.

RKB zapewnia ochronę:

- informacji przetwarzanych w RChO w tym zasobów systemów wewnętrznych administracji oraz e-usług świadczonych przez Internet;
- punktu styku z Internetem, uwzględniając odpowiednie wytyczne co do ilości operatorów świadczących usługę oraz sposobu zapewnienia na poziomie operatorskim zabezpieczenia przed atakami wolumetrycznymi;
- punktu styku ww. infrastruktury z wewnętrznymi sieciami rządowymi – uwaga sieci te świadczą wrażliwe usługi dla podmiotów administracji centralnej w zakresie ochrony bezpieczeństwa publicznego.

Z uwagi na konieczność zapewnienia bezpieczeństwa teleinformatycznego szczegóły architektury bezpieczeństwa projektu ROZBUDOWA KATALOGU USŁUG RZĄDOWEJ CHMURY OBLICZENIOWEJ (ROZBUDOWA\_RCHO) nie zostaną ujawnione.