

OPIS ZAŁOŻEŃ PROJEKTU INFORMATYCZNEGO

Tytuł projektu	Centrum Reputacyjne Komunikacji Elektronicznej (CRKE)		
Wnioskodawca	Minister Cyfryzacji		
Beneficjent	Urząd Komunikacji Elektronicznej		
Partnerzy	Nie dotyczy		
Źródło finansowania	84,63% dofinansowanie UE (II oś POPC E-administracja i otwarty rząd; Działanie 2.1 Wysoka dostępność i jakość usług publicznych); 15,37% dofinansowanie z budżetu Państwa - część budżetowa nr 76 (dysponent: Prezes UKE).		
Całkowity koszt projektu	24 000 000,00 zł		
Planowany okres realizacji projektu	03-2022 do 11-2023		
Osoba kontaktowa	Daniel Kraszewski	Daniel.Kraszewski@uke.gov.pl	532540226

1. POWODY PODJĘCIA PROJEKTU

1.1. Identyfikacja problemu i potrzeb

System CRKE umożliwi Prezesowi UKE realizację określonego ustawą Prawo Telekomunikacyjne obowiązku podejmowania interwencji w sprawach dotyczących funkcjonowania rynku usług telekomunikacyjnych i pocztowych oraz rynku aparatury, w tym rynku urządzeń telekomunikacyjnych, z własnej inicjatywy lub wniesionych przez zainteresowane podmioty, w szczególności użytkowników i przedsiębiorców telekomunikacyjnych, w tym podejmowania decyzji w tych sprawach w zakresie określonym ww. ustawą oraz rozpatrywania skarg. Jednocześnie, System stanowi odpowiedź na potrzebę wzmocnienia kompetencji, pozwalających na identyfikację zdarzeń lub incydentów, wpływających na reputację komunikacji elektronicznej, a w efekcie na konsumenta.

Efektywne działanie we wskazanym obszarze wymaga zbudowania systemu, który pozwoli realizować Prezesowi UKE wskazane obowiązki.

Problem zabezpieczenia systemowego przed zagrożeniami bezpieczeństwa sieci dotyczy zarówno klientów indywidualnych jak i przedsiębiorców. Systemowe rozwiązanie w postaci CRKE pozwoli interesariuszom pozyskać wiedzę w celu minimalizacji ryzyk związanych z komunikacją elektroniczną.

Na etapie opracowywania założeń projektu przeprowadzono konsultacje z grupą podmiotów, należących do przedstawicieli izb branżowych zrzeszających PT, jak i indywidualnych PT, łącznie kilkaset podmiotów z branży. Wynikiem tych konsultacji jest zawarte „Porozumienie w sprawie współpracy w zakresie bezpieczeństwa teleinformatycznego” z 4 największymi operatorami sieci mobilnych tj.: Orange, Play, Plus i T-Mobile. W spotkaniach organizowanych w ramach ww. porozumienia uczestniczą również przedstawiciele KGP, IŁ-PIB i NASK a ich efektem jest propozycja legislacyjna dotycząca zapobiegania phishingowi oraz prace w zakresie zwalczania spoofingu.

Przedstawione założenia projektu wpisują się w realizację zadań UKE wskazanych w ustawie Prawo telekomunikacyjne (art. 101 ust. 2, art. 189 ust. 2 pkt 3 lit. f oraz art. 192 ust. 1 pkt 5 i 9 oraz 13).

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
Przedsiębiorcy telekomunikacyjni (w szczególności z sektora MŚP)	<ol style="list-style-type: none"> 1. Brak możliwości bezpiecznej wymiany doświadczeń, dzielenia się wiedzą o incydentach między Przedsiębiorcami Telekomunikacyjnymi (PT). 2. Potrzeba wymiany doświadczeń i wniosków, dotyczących narzędzi i taktyk pozwalających na wczesną detekcję i blokowanie incydentów związanych z bezpieczeństwem sieci i unikanie incydentów w sieciach telekomunikacyjnych. 3. Brak możliwości efektywnego przeprowadzenia diagnozy poziomu bezpieczeństwa, identyfikacji słabości w bezpieczeństwie oraz skutecznego wdrażania, rekomendacji przez PT w ich sieciach. 4. Zróżnicowany poziom świadomości bieżących zagrożeń w zależności od potencjału PT. 5. Zróżnicowany poziom dojrzałości organizacji w obszarze bezpieczeństwa sieci. 6. Znaczna liczba podatności mogących wpływać na bezpieczeństwo sieci i usług dostarczanych przez PT 7. Brak zaufania i niski poziom współpracy oraz wymiany informacji pomiędzy konkurującymi między sobą PT 	4 124 przedsiębiorców telekomunikacyjnych
Klienci (indywidualni oraz instytucjonalni) przedsiębiorców telekomunikacyjnych	<ol style="list-style-type: none"> 1. Brak możliwości rozpatrywania przez UKE w ramach e – usługi interwencji i skarg dotyczących m.in. zakłóceń i incydentów w zakresie bezpieczeństwa i integralności sieci 2. Brak informacji o reputacji i stanie sieci, poziomie dostępności, ciągłości usług telekomunikacyjnych. 3. Zakłócenia/incydenty w zakresie bezpieczeństwa, prywatności i/lub integralności mające miejsce, lub pochodzące ze słabo zabezpieczonych sieci teleinformatycznych o niskiej reputacji mogą mieć negatywny wpływ na jakość / ciągłość usług oferowanych klientom indywidualnym oraz finalnie na reputację usług telekomunikacyjnych. 	16,2 mln użytkowników sieci Internet; liczba aktywnych kart SIM -52,2 mln szt 3,5 mln abonentów telefonii stacjonarnej; 2,5 mln abonentów / użytkowników VoIP
Stowarzyszenia zrzeszające przedsiębiorców telekomunikacyjnych	Brak możliwości bezpiecznego transferu wiedzy i informacji na temat poziomu nieautoryzowanego ruchu w sieci, oraz narzędzi do weryfikacji sporów między przedsiębiorcami co do rozliczeń usług w sieciach.	4

1.2. Opis stanu obecnego

W 2020 r. UKE odnotował ponad 5700 interwencji i skarg, w tym 96 dotyczyło poważnych naruszeń bezpieczeństwa i integralności sieci i usług (w 2019 r. odnotowano 95 tego typu naruszeń, a w 2018 r. - 198). Natomiast w 2019 r. CERT Polska obsłużył łącznie 22343 zgłoszenia. Na podstawie 10489 zgłoszeń zarejestrowano 6 484 incydenty (dla porównania w 2018 r. - 3739 incydentów). W porównaniu do danych za 2018 r. zarejestrowano rekordowy wzrost liczby obsługiwanych incydentów na poziomie 73%. Powyższe dane obrazujące zgłoszenia raportowane do UKE czy CERT Polska mogą nie obejmować wszystkich naruszeń przez co skala i skutki incydentów w sektorze Telco mogą być znacząco większe. Zjawiska te będą się nasilać, uwzględniając postępującą rozbudowę sieci i rozwój usług. Na dzień dzisiejszy brak jest systemu, który obsługiwany przez jeden podmiot (UKE) pozwoli na rozpatrywanie interwencji i skarg obywateli oraz przekazywanie informacji do właściwych podmiotów w celu podjęcia przez nie odpowiednich działań, jeżeli będą one leżały w ich kompetencjach. PT identyfikują naruszenia bezpieczeństwa oraz integralności sieci lub usług na podstawie kryteriów mających istotny wpływ na funkcjonowanie sieci lub usług telekomunikacyjnych, które dotknęły co najmniej 10000 użytkowników przez określony czas. Zgłoszeniu podlegają również naruszenia skutkujące niedostępnością telefonów alarmowych. Ponadto pojawia się wiele niepokojących informacji o różnego rodzaju aktywnościach z wykorzystaniem połączeń telefonicznych oraz SMS, mogących prowadzić do strat finansowych u konsumentów (nakłanianie do instalacji szkodliwych aplikacji, powodujących kradzież danych oraz środków finansowych, czy wiadomości SMS zachęcające do zapoznania się z „ofertą”, a w efekcie aktywujące niechciane płatne usługi bez wiedzy konsumenta). UKE obecnie nie posiada narzędzia zapewniającego m.in. automatyczną identyfikację zdarzeń lub incydentów, wpływających na reputację komunikacji elektronicznej, a w efekcie na konsumenta.

2. EFEKTY PROJEKTU

2.1. Cele i korzyści wynikające z projektu

Cel - 1	Poszerzenie zakresu spraw, które obywatele i przedsiębiorcy mogą załatwić drogą elektroniczną a w efekcie zwiększenie dostępności i jakości e-usług publicznych.
Cel strategiczny	<p>Przedmiotowy projekt wpisuje się w następujące dokumenty strategiczne:</p> <p>1/ Program Zintegrowanej Informatyzacji Państwa, cel główny: modernizacja administracji publicznej i usprawnienie funkcjonowania państwa przy wykorzystaniu technologii cyfrowych cel szczegółowy: Zwiększenie jakości oraz zakresu komunikacji między obywatelami i innymi interesariuszami a państwem (o którym mowa w pkt 4.2.1 Programu),</p> <p>2/ Program Operacyjny Polska Cyfrowa, cel szczegółowy nr 2 „Wysoka dostępność i jakość e-usług publicznych” w ramach Osi priorytetowej II. „E-administracja i otwarty rząd” PO PC,</p> <p>3/ Strategia na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.) Obszar: E-państwo / Kierunek Interwencji: Budowa i rozwój e-administracji – orientacja administracji państwa na usługi cyfrowe</p> <p>4/ „Strategiczne kierunki działań Prezesa UKE w latach 2017-2021”. Kierunek: podnoszenie jakości usług telekomunikacyjnych, w tym zapewnienie ich bezpieczeństwa, m.in. poprzez promowanie rekomendacji i standardów ENISA (European Union Agency for Cybersecurity) oraz wdrażanie dobrych</p>

	praktyk w zakresie cyberbezpieczeństwa przez regulatorów UE, 5/ „Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024”. Cel szczegółowy 1 – rozwój krajowego systemu cyberbezpieczeństwa.
Korzyść:	<p>1/ Minimalizacja kosztów związanych z skutkami i obsługą zgłoszonych interwencji i skarg wnoszonych do UKE przez użytkowników.</p> <p>2/ Zwiększenie zaufania do usług zarządzanych i udostępnianych przez administrację państwową dzięki możliwości sprawnej obsługi zgłoszeń oraz udostępnianiu informacji dotyczących wskaźników reputacji.</p> <p>3/ Poprawa jakości i niezawodności cyfrowych usług publicznych oraz możliwość świadczenia ich bardziej zaawansowanych form.</p> <p>4/ Podniesienie poziomu bezpieczeństwa sieci i usług w sektorze Telco.</p> <p>5/ Umożliwienie bezpiecznej wymiany informacji z i pomiędzy PT w zakresie obszaru bezpieczeństwa sieci i usług oferowanych przez PT pozwalającej na zacieśnienie współpracy pomiędzy specjalistami ds. bezpieczeństwa PT, a innymi podmiotami o podobnych funkcjach.</p> <p>6/ Wypracowanie i propagacja rekomendacji w zakresie bezpieczeństwa usług telekomunikacyjnych w oparciu o rekomendacje CSIRT Poziomu Krajowego oraz analogicznych źródeł, rekomendacje dla Telco.</p> <p>7/ Minimalizacja kosztów związanych ze skutkami i obsługą incydentów bezpieczeństwa zarówno w odniesieniu do klienta indywidualnego jak i podmiotów administracji państwowej.</p>
KPI:	<p>KPI nr 1: Liczba usług publicznych udostępnionych on-line o stopniu dojrzałości co najmniej 4 – transakcja</p> <p>KPI nr 2: Liczba załatwionych spraw poprzez udostępnioną on-line usługę publiczną</p> <p>KPI nr 3: Liczba uruchomionych systemów teleinformatycznych w podmiotach wykonujących zadania publiczne</p> <p>KPI nr 4: Liczba pracowników podmiotów wykonujących zadania publiczne niebędących pracownikami IT, objętych wsparciem szkoleniowym – ogółem</p> <p>KPI nr 5: Liczba pracowników podmiotów wykonujących zadania publiczne nie będących pracownikami IT, objętych wsparciem szkoleniowym – kobiety</p> <p>KPI nr 6: Liczba pracowników podmiotów wykonujących zadania publiczne nie będących pracownikami IT, objętych wsparciem szkoleniowym – mężczyźni</p>
Wartość aktualna i docelowa KPI:	<p>wartość bazowa KPI nr 1: 0</p> <p>wartość bazowa KPI nr 2: 0</p> <p>wartość bazowa KPI nr 3: 0</p> <p>wartość bazowa KPI nr 4: 0</p> <p>wartość bazowa KPI nr 5: 0</p> <p>wartość bazowa KPI nr 6: 0</p> <p>wartość docelowa KPI nr 1: 1</p> <p>wartość docelowa KPI nr 2: 7 600</p> <p>wartość docelowa KPI nr 3: 1</p> <p>wartość docelowa KPI nr 4: 32</p> <p>wartość docelowa KPI nr 5: 16</p> <p>wartość docelowa KPI nr 6: 16</p>
Metoda pomiaru KPI	<p>Metoda, źródło danych i częstotliwość pomiaru KPI nr 1: testy wdrożeniowe i akceptacyjne systemu zakończone Odbiorem Końcowym systemu, pomiar jednokrotny na koniec realizacji projektu.</p> <p>Metoda i częstotliwość pomiaru KPI nr 2: statystyczne raporty systemowe przedstawiające liczbę załatwionych spraw, pomiar kwartalny, po zakończeniu</p>

	<p>proiektu, w okresie trwałości projektu.</p> <p>Metoda i częstotliwość pomiaru KPI nr 3: Protokół Odbioru Końcowego systemu, pomiar jednokrotny na koniec realizacji projektu.</p> <p>Metoda i częstotliwość pomiaru KPI nr 4, 5, 6: dokumentacja szkoleniowa – listy obecności, wyniki testów wiedzy i umiejętności po szkoleniu, pomiar jednokrotny na koniec realizacji projektu.</p>
--	--

2.2. Udostępnione e-usługi

Lp.	Nazwa e-usługi	Typ	Zakres oddziaływania	Poziom dojrzałości e-usługi
1	Usługa automatycznego przekazywania i rozpatrywania zgłoszonych interwencji i skarg wnoszonych do UKE przez użytkowników sieci	A2B A2C	Przedsiębiorcy telekomunikacyjni (w szczególności z sektora MŚP) Klienci (indywidualni oraz instytucjonalni) przedsiębiorców telekomunikacyjnych Stowarzyszenia zrzeszające przedsiębiorców telekomunikacyjnych (rocznie ok 7600 transakcji)	Personalizacja

2.3. Udostępnione informacje sektora publicznego i zdigitalizowane zasoby

Rodzaj informacji/zasobów	Planowana data udostępnienia	Szacowana liczba obiektów objętych digitalizacją (udostępnianiem informacji)
informacje statystyczne dotyczące zgłoszonych interwencji i skarg wnoszonych do UKE przez użytkowników sieci	04-09-2023	1
dokumentacja API integracyjna	04-09-2023	3

Czy wszystkie zdigitalizowane zasoby objęte projektem będą udostępniane bezpłatnie?
TAK/NIE

2.4. Produkty końcowe projektu

Nazwa produktu	Planowana data wdrożenia
System CRKE	11-2023
Usługa automatycznego przekazywania i rozpatrywania zgłoszonych interwencji i skarg wnoszonych do UAE przez użytkowników sieci	11-2023
Informacje statystyczne dotyczące zgłoszonych interwencji i skarg wnoszonych do UAE przez użytkowników sieci	11-2023
Dokumentacja API integracyjna (3 obszary: PT, Konsumenci, KSC)	11-2023
Materiały promocyjne	11-2023
Materiały szkoleniowe	11-2023

3. KAMIENIE MIŁOWE

Kamienie milowe	Planowany termin osiągnięcia
Opracowana specyfikacja docelowego rozwiązania systemu CRKE.	2022-04-25
Dostarczona platforma sprzętowa oraz oprogramowanie wraz z instalacją fizyczną.	2022-08-29
Skonfigurowany system VM wraz z integracją.	2022-09-12
Uruchomiony prototyp platformy narzędziowej dla CRKE.	2023-03-13
Wdrożone scenariusze analityczne (rozwój systemu CRKE).	2023-07-31
Zakończone testy systemu CRKE.	2023-09-04
Przedstawienie Systemu CRKE do Odbioru Końcowego.	2023-09-04
Zrealizowane szkolenia.	2023-09-18
Odebrany System CRKE.	2023-10-30

4. KOSZTY

4.1. Koszty ogólne projektu wraz ze sposobem finansowania

Całkowity koszt projektu (netto oraz brutto), w tym	Netto 19 512 195,12 zł Brutto 24 000 000,00 zł	
Procent dofinansowania ze środków UE (brutto)	84,63%	
Procent środków z budżetu państwa (brutto)	15,37%	
Podział całkowitego kosztu projektu na poszczególne lata (netto oraz brutto)	2022	Netto 8 739 837,40 zł Brutto 10 750 000,00 zł
	2023	Netto 10 772 357,72 zł Brutto 13 250 000,00 zł

4.2. Wykaz poszczególnych pozycji kosztowych

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
Oprogramowanie	Oprogramowanie obejmuje niezbędne narzędzia i oprogramowanie zabezpieczające działanie e-usługi.	12 500 000,00 zł	Oprogramowanie to jeden z niezbędnych elementów do funkcjonowania systemu CRKE (w szczególności w postaci e-usługi).
Infrastruktura	Infrastruktura techniczna niezbędna do implementacji rozwiązania	2 700 000,00 zł	Infrastruktura techniczna niezbędna do implementacji rozwiązania oraz narzędzia wspierające administrowanie systemem, w tym narzędzia do zarządzania użytkownikami tj. wynajem infrastruktury (usługi IaaS) oraz zespół administracyjno-devopsowy.
Koszty UX i grafiki	Zapewnienie przyjaznego oraz ergonomicznego interfejsu z punktu widzenia użytkowników systemu.	750 000,00 zł	W celu zapewnienia odpowiedniej ergonomii użytkownika, intuicyjnego GUI w architekturze klient-serwer i wsparcia różnych OS (Windows, Android, IOS), w tym aplikacje wizualizacji wyników i aktywny dashboard.
Bezpieczeństwo	opracowanie / zakup elementów gwarantujących bezpieczeństwo systemu	2 400 000,00 zł	opracowanie / zakup elementów gwarantujących bezpieczeństwo systemu
Wydajność	Koszt obejmuje	580 000,00 zł	Przygotowanie koncepcji CRKE,

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
rozwiązań	realizację głównych procesów jakie mają doprowadzić do docelowego rozwiązania		obejmuje projekt techniczny, funkcjonalny i organizacyjny oraz opracowanie prototypu platformy. Implementacja rozwiązania wraz ze wszystkimi komponentami technologicznymi, aplikacyjnymi oraz elementami bezpieczeństwa. W ramach platformy, zostanie wytworzony autorski system.
Szkolenia	Szkolenia skierowane zarówno do administratorów i przygotowania zespołów, jak i szkolenia dla użytkowników	500 000,00 zł	Szkolenia osób zaangażowanych w obsługę systemu, niezbędne do efektywnego wdrożenia efektów projektu.
Działania informacyjno-promocyjne	content marketing, konferencja, publikacje w czasopismach i na portalach branżowych	970 000,00 zł	Są to działania niezbędne do by do rozpowszechnienia efektów uzyskanych w ramach realizacji projektu wśród docelowej grupy odbiorców.
Koszty zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego)	wynagrodzenia osób zaangażowanych w realizację projektu	3 600 000,00 zł	wynagrodzenia osób zaangażowanych w realizację projektu brutto-brutto (obejmujące także składki ubezpieczeniowe opłacane przez pracodawcę); koszty nie przekraczają 15% całkowitej wartości projektu.

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

Całkowity koszt utrzymania trwałości projektu (brutto)	2 417 709,59 zł		Źródło finansowania
Podział całkowitego kosztu utrzymania trwałości projektu na poszczególne lata (netto oraz brutto)	2023	19 709,59 zł (brutto) (16 024,06 zł netto)	krajowe środki publiczne - budżet państwa
	2024	479 600,00 zł (brutto) (389 918,70 zł netto)	krajowe środki publiczne - budżet państwa

	2025	479 600,00 zł (brutto) (389 918,70 zł netto)	krajowe środki publiczne - budżet państwa
	2026	479 600,00 zł (brutto) (389 918,70 zł netto)	krajowe środki publiczne - budżet państwa
	2027	479 600,00 zł (brutto) (389 918,70 zł netto)	krajowe środki publiczne - budżet państwa
	2028	479 600,00 zł (brutto) (389 918,70 zł netto)	krajowe środki 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
Brak możliwości właściwej identyfikacji zgłoszonej sprawy	Średnia	Średnie	Bieżące monitorowanie zgłoszonych spraw. Opracowanie optymalnych procedur działania.
Błędna ocena czynników ryzyka	Duża	Średnie	Do identyfikacji czynników zostaną wykorzystane zróżnicowane źródła wiedzy o bezpieczeństwie systemu, w tym aktualne zbiory charakterystyk ataków teleinformatycznych pochodzące m.in. od przedsiębiorstw telekomunikacyjnych.
Nieodpowiednie zabezpieczenie przetwarzanych i wykorzystywanych danych w pracach nad budową i rozwojem	Duża	Niskie	Opracowanie zaleceń w zakresie bezpiecznego przetwarzania danych (anonimizacja danych, kontrola dostępu). Przeszkolenie zaangażowanego personelu w zakresie bezpieczeństwa danych.

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
systemu.			Stosowanie pseudonimizacji danych testowych. Użycie generatorów danych do zastosowania podczas testów. Cykliczne monitorowanie środowiska bezpieczeństwa.
Nadmierna rotacja członków zespołu projektowego	Średnia	Średnie	Prowadzenie repozytorium projektowego, w którym umieszczane będą wszelkie informacje o stanie poszczególnych zadań oraz dokumenty związane z nimi. Wykorzystywanie systemu motywowania w celu utrzymania stałego zespołu. Monitorowanie nastrojów zespołu w celu aktywnego oddziaływania. Bieżące rozwiązywanie problemów projektowych i wewnątrz zespołowych.
Nieosiągnięcia ostatniego kamienia milowego w okresie kwalifikowalności wydatków w perspektywie finansowej 2014-2020.	Średnia	Niskie	Wsparcie eksperckie przy opracowaniu specyfikacji zamówienia publicznego oraz w dalszych częściach realizacji umowy z wykonawcą, priorytetowa pomoc prawna na każdym etapie zamówienia publicznego do czasu wykonania umowy, bieżące monitorowanie realizacji kamieni milowych przez kierownika projektu i podejmowanie bieżących usprawnień i działań mitygujących ryzyko.

5.2. Ryzyka wpływające na utrzymanie efektów

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Niekonkurencyjność w miarę upływu czasu	Duża	Niskie	W pracach nad rozwiązaniem konieczne będzie uwzględnienie w analizie zagrożeń różnych modeli: działanie ludzi, urządzeń czy sieci. Elementem wpływającym na zmniejszenie tego typu ryzyka jest również analiza danych ze wszystkich dostępnych źródeł oraz ciągłe uczenie się i porównania do normalnie działającej sieci, korelacja wszelkich anomalii. Monitorowanie

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
			metod dostępnych w istniejących rozwiązaniach. Monitorowanie wskaźników . Konsultacja metod w ramach sieci ISAC.
Zmiany legislacyjne warunkujące zmiany w działaniu Systemu CRKE	Średnia	Średnie	Bieżący monitoring zmian prawnych oraz dostosowywanie organizacyjnotechniczne CRKE uwzględniające nowe regulacje prawne. Wymiana informacji w ramach na zasadach ISAC.
Niewystarczająca liczba użytkowników końcowych Systemu zainteresowanych skorzystaniem z e-usługi	Średnia	Średnie	Przygotowanie kampanii informacyjnej dotyczącej branżowych zagadnień związanych z potrzebą monitorowania infrastruktury IT. Kontakty bezpośrednie z przedsiębiorcami telekomunikacyjnymi zaangażowanymi w projekt dla informowania innych podmiotów w ramach kontaktów branżowych.

6. OTOCZENIE PRAWNE

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
1	Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. 2004 nr 171 poz. 1800, ze zmianami)	TAK/NIE		
2	Ustawa z dnia ... wprowadzająca ustawę – Prawo komunikacji elektronicznej – Projekt z dnia 29 lipca 2020 r. https://legislacja.gov.pl/projekt/12336501	TAK/NIE		
3	Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560)	TAK/NIE		
4	Ustawa z dnia ... 2020 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych - Projekt z 7 września 2020 r. https:// mc.bip.gov.pl/articles/view/361169/projektustawy-o-zmianie-ustawy-o-krajowym-systemiecyberbezpieczenstwa-oraz-ustawy-prawozamowien-publicznych.html/year:2020/	TAK/NIE		

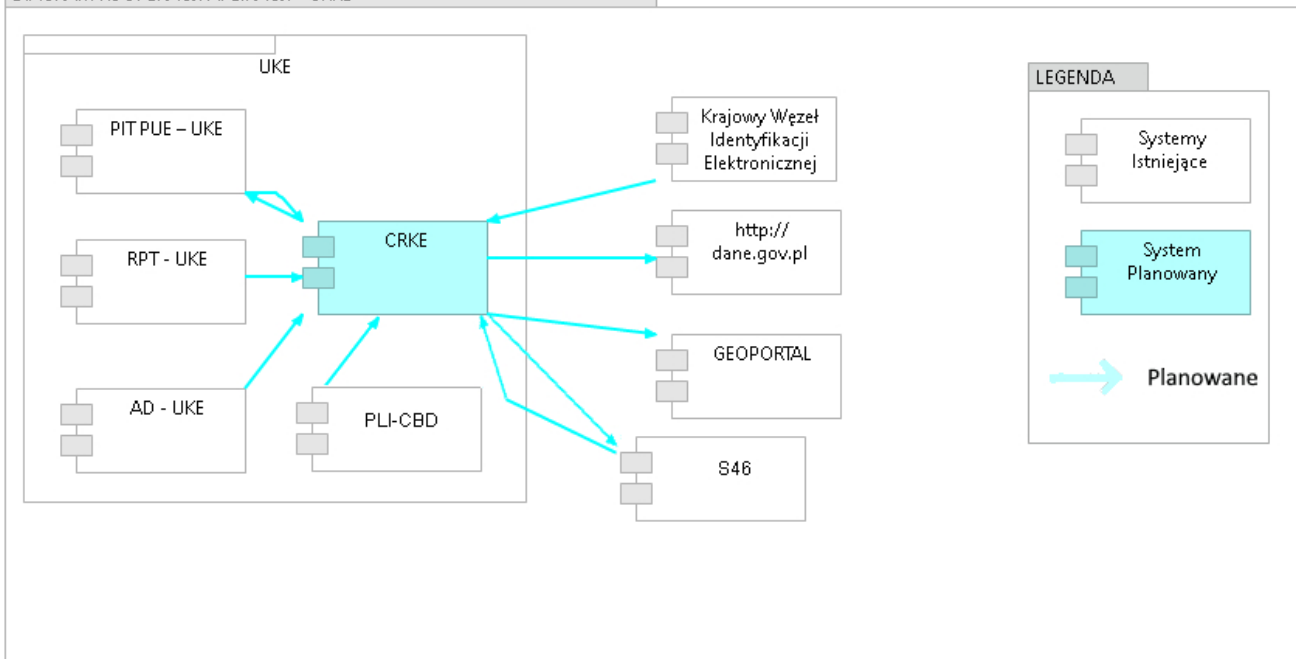
Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
	month:09/day:08			
5	Rozporządzenie Ministra Cyfryzacji z dnia 22 czerwca 2020 r. w sprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług. (Dz. U. 2020 poz. 1130.)	TAK/NIE		
6	Rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie wzoru formularza do przekazywania informacji o naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych, które miało istotny wpływ na funkcjonowanie sieci lub usług. (Dz. U. 2018 poz. 1831)	TAK/NIE		
7	Rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług (Dz. U. 2018 poz. 1830)	TAK/NIE		
8	Rozporządzenie Rady Ministrów z dnia 19 sierpnia 2020 r. w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń. (Dz. U. 2020 poz. 1464)	TAK/NIE		
9	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 26.11.2015 PL Dziennik Urzędowy Unii Europejskiej L 310/1)	TAK/NIE		
10	DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (17.12.2018 PL Dziennik Urzędowy Unii Europejskiej L 321/36)	TAK/NIE		
11	DYREKTYWA 2007/2/WE PARLAMENTU EUROPEJSKIEGO I RADY z dnia 14 marca 2007 r. ustanawiająca infrastrukturę informacji przestrzennej we Wspólnocie Europejskiej	TAK/NIE		

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
	(INSPIRE) (25.4.2007 PL Dziennik Urzędowy Unii Europejskiej L 108/1)			
12	Komunikat KE łączności dla konkurencyjnego jednolitego rynku cyfrowego „W kierunku społeczeństwa gigabitowego”- cele do 2025 r. https://www.gov.pl/web/cyfryzacja/komunikatkomisji-europejskiej-w-kierunku-europejskiegospolesctwa-gigabitowego	TAK/NIE		
13	Europejska Agenda Cyfrowa https://www.europarl.europa.eu/factsheets/pl/sheet/64/digital-agenda-for-europe	TAK/NIE		
14	BEREC Opinion for the evaluation of the application of Regulation (EU) 2015/2120 and the BEREC Net Neutrality Guidelines, BOR(18)244, 6.12.2018 https://berec.europa.eu/eng/document_register/subject_matter/berec/opinions/8317%20berec-opinion-for-the-evaluation-of-theapplication-of-regulation-eu-20152120-and-theberec-netneutrality-guidelines	TAK/NIE		
15	ROZPORZĄDZENIE RADY MINISTRÓW z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20170002247/O/D20172247.pdf	TAK/NIE		
16	Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne z późn. zm.	TAK/NIE		

7. ARCHITEKTURA

7.1. Widok kooperacji aplikacji

DIAGRAM KOOPERACJI APLIKACJI - CRKE



Lista systemów wykorzystywanych w projekcie

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
1	CRKE	Regulator - UKE	System zawierający planowaną e-usługę	Planowany	
2	Krajowy Węzeł Identyfikacji Elektronicznej	KPRM	Krajowy Węzeł Identyfikacji Elektronicznej (login.gov.pl) pośredniczy w uwierzytelnianiu w krajowych usługach online za pomocą środków identyfikacji elektronicznej wydanych przez różne podmioty w ramach systemów identyfikacji elektronicznej.	Istniejący	
3	Dane.gov.pl	KPRM	Portal Centralnego Repozytorium Informacji Publicznej, wskazanego w Ustawie o dostępie do informacji publicznej (Dz. U. Nr 112, poz. 1198, z późn. zm.) jako jeden z trybów dostępu i ponownego wykorzystywania	Istniejący	

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			informacji publicznej.		
4	Active Directory (AD)	Regulator - UKE	System podstawowej rejestracji i logowania klientów UKE.	Istniejący	
5	Rejestr Przedsiębiorców Telekomunikacyjnych – RPT	Regulator - UKE	System informatyczny obsługujący rejestr o którym mowa w Art. 10 ustawy Prawo Telekomunikacyjne.	Istniejący	
6	GEOPORTAL / Dane centralnego zasobu geodezyjnego i kartograficznego	GUGiK	<p>Geoportal krajowy to aplikacja internetowa umożliwiająca przeglądanie danych przestrzennych oraz wyszukiwanie zbiorów i usług danych przestrzennych należących do Krajowej Infrastruktury Informacji Przestrzennej.</p> <p>Aplikacja dostępna jest pod adresem: http://mapy.geoportal.gov.pl/.</p> <p>Dane publikowane w ramach Geoportalu krajowego są przechowywane w Państwowym Zasobie Geodezyjnym i Kartograficznym (PZGiK).</p> <p>W projekcie wykorzystane zostaną:</p> <ul style="list-style-type: none"> Osnowy geodezyjne, grawimetryczne i magnetyczne Państwowy rejestr granic i jednostek podziałów terytorialnych kraju Ortofotomapa Mapy topograficzne Państwowy Rejestr Nazw Geograficznych Dane pomiarowe Numeryczny model terenu Numeryczny model pokrycia terenu Mapy tematyczne Baza Danych Obiektów Ogólnogeograficznych 	Istniejący	

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			Zintegrowane kopie baz danych obiektów topograficznych BDOT10k Zobrazowania lotnicze		
7	PIT-PUE	Regulator - UKE	Punkt Informacyjny ds. Telekomunikacji (PIT) 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. W projekcie w szczególności zostaną wykorzystane dane skojarzone z krajową bazą danych geodezyjnej ewidencji sieci uzbrojenia terenu prowadzonej przez Głównego Geodetę Kraju oraz z e-usług prezentujących informacje z powiatowych baz geodezyjnej ewidencji sieci uzbrojenia terenu.	Istniejący	
8	PLI CBD	Regulator - UKE	System pozyskiwania informacji o lokalizacji abonenta wzywającego pomocy (pod numery alarmowe, w tym 112) oraz usprawnienie procesów związanych z przenoszeniem numerów przy zmianie operatora.	Istniejący	
9	S46	NASK PIB	System S46 udostępnia informacje zespołom SOC operatorów usług kluczowych i innym podmiotom krajowego systemu cyberbezpieczeństwa.	Istniejący	

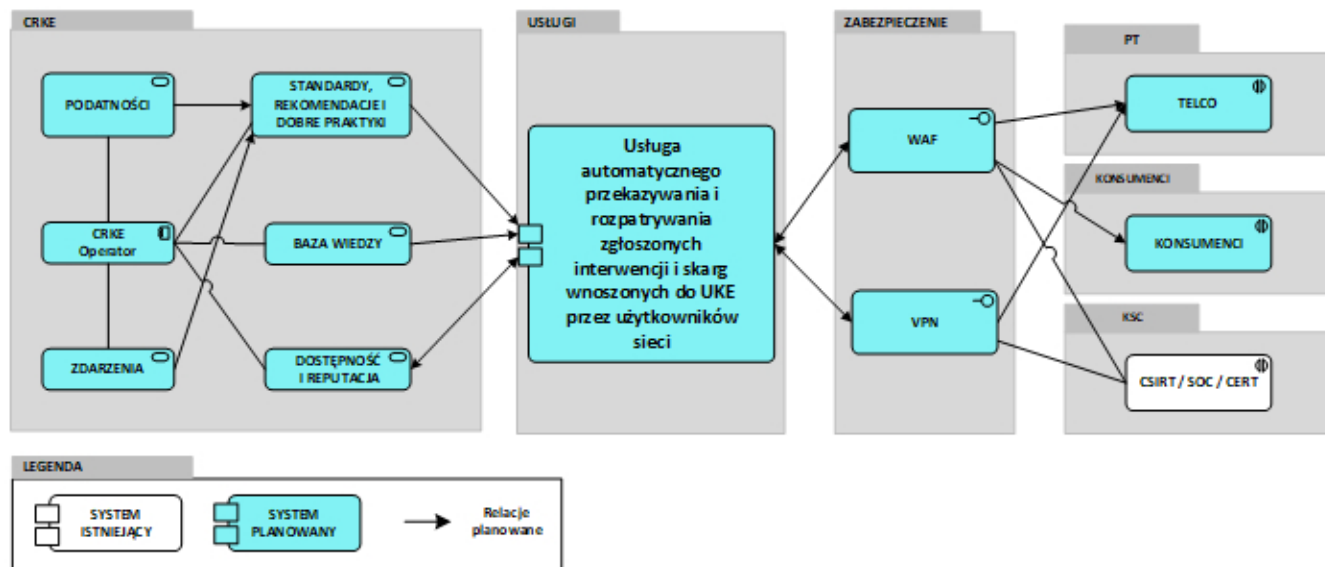
Lista przepływów

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
1	PIT PUE UKE	CRKE	Komunikacja z interesariuszami. Zgłoszenia incydentów, zdarzeń bezpieczeństwa.	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
2	CRKE	PIT PUE UKE	Diagnoza poziomu bezpieczeństwa, informacje o identyfikacji słabości w bezpieczeństwie testowanej infrastruktury i aplikacji, zalecenia, wytyczne, informacje o ruchu w sieci PT. Informacje o zakłóceniach incydentach w zakresie bezpieczeństwa i/lub integralności, informacje o reputacji sieci teleinformatycznych	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
3	RPT	CRKE	Dane o Przedsiębiorcach Telekomunikacyjnych w kraju wraz z zakresem i parametrach świadczonych przez nich	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

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
			usług			
4	AD-UKE	CRKE	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 UKE – standard HTTPS
5	Krajowy Węzeł Identyfikacji Elektronicznej	CRKE	Dane związane z tożsamością użytkownika systemu (Nazwisko, Imię, Data urodzenia, NIP, PESEL, Data urodzenia)	Inicjowany przez podmiot zewnętrzny posiadający PZ	Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych UKE – standard HTTPS, SOAP
6	CRKE	http://dane.gov.pl	Prezentacja raportów z e-usług cyfrowych	Automatyczny dla raportów okresowych lub inicjowany przez pracownika UKE z wykorzystaniem udostępnionych mechanizmów (API) Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych UKE i zewnętrznych – standard HTTPS
7	CRKE	GEOPORTAL	Prezentacja obiektów i informacji systemowych na mapach	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

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
8	CRKE	S46	Informacje bieżące , Informacje pozyskane z sieci, MISP,	Dla wszystkich systemów wewnętrznych UAE i zewnętrznych: przez Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów Wewnętrznych UAE i zewnętrznych -standard HTTPS, JSON, MISP
9	S46	CRKE	Informacje bieżące, podatności, dobre praktyki, rekomendacje , informacje o incydentach, MISP	Dla wszystkich systemów wewnętrznych UAE i zewnętrznych: przez Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych UAE i zewnętrznych -standard HTTPS, JSON, MISP
10	PLI-CBD	CRKE	Informacje o usterkach zgłaszanych przez operatorów uczestniczących w procesie przenoszenia numerów, Informacje od „małych operatorów” dot, przekazywania oraz kontroli wymaganych danych.	Dla wszystkich systemów wewnętrznych UAE i zewnętrznych: przez Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Tryb odwołań bezpośrednich (§13 ust. 2) KRI	Dla wszystkich systemów wewnętrznych UAE i zewnętrznych -standard HTTPS, JSON, MISP

7.2. Kluczowe komponenty architektury rozwiązania



7.3. Przyjęte założenia technologiczne

Lp.	Obszar	Założenie technologiczne
1.	Infrastruktura	Infrastruktura oparta o istniejące technologie serwerowe, bazodanowe i macierzowe
2.	Sieć i bezpieczeństwo	Sieć gigabit ethernet, FC, protokoły wymiany danych zgodne z TLS v.1.3 lub odpowiednie, system klasy WAF, system Firewall z funkcją IDS/IPS
3.	Standardy wymiany danych	Sieć IP z zapewnieniem odpowiedniego szyfrowania
4.	Systemy operacyjne serwerowe	Głównie systemy z rodziny Linux
5.	Bazy danych	MySQL, natywne systemy bazodanowe dla rozwiązań bezpieczeństwa, indeksy Elasticsearch, Hadoop
6.	Serwery aplikacji	Apache
7.	Portale	
8.	Inne	

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

Projektowana struktura CRKE będzie poprzez rozwiązania architektoniczne spełniała wysokie standardy m.in. jeśli chodzi o zapewnienie ciągłości działania, jako dostawca szeregu usług oferowanych w reżimie 24/7, oraz standardy bezpieczeństwa i ochrony informacji, które w momencie uruchomienia na koniec projektu potwierdzone zostaną pozyskaniem certyfikatów: PN-ISO/IEC 22301 - z zakresie systemu zarządzania ciągłością działania w zakresie świadczenia usług związanych z sieciami teleinformatycznymi i cyberbezpieczeństwem, PN-ISO/IEC 24762 - w zakresie systemu i procesu odtwarzania zasobów IT po katastrofie w ramach odtwarzania komponentów niezbędnych do zapewnienia ciągłości działania. ISO 27001 - w zakresie systemu zarządzania bezpieczeństwem informacji w zakresie świadczenia usług związanych z sieciami teleinformatycznymi i cyberbezpieczeństwem.

Całość platformy teleinformatycznej zbudowanej dla potrzeby CRKE, będzie spełniać wysokie standardy procesów utrzymania komponentów IT w działaniu, obejmujące takie cykliczne procesy jak:

- bieżące aktualizacje komponentów oprogramowania, pod kątem podatności, aktualności wersji, polityki uwierzytelniania tworzenia i zmiany haseł, kontroli i hierarchii dostępu, bezpieczeństwa i archiwizacji przechowywania danych.
- kontrola efektywności i kompleksowości mechanizmów redundancji, dostępu do oprogramowania systemowego, aktualizacje oprogramowania systemowego pod kątem usuwania luk i aktualizacji jego wersji, zapewnienia pełnej kontroli na fizycznym dostępem do fizycznych komponentów architektury.