OPIS ZAŁOŻEŃ PRZEDSIĘWZIĘCIA INFORMATYCZNEGO

Tytuł przedsięwzięcia	Bezpieczna komunikacja mobilna dla podmiotów KSC (BKM)		
Wnioskodawca	Minister Cyfryzacji		
Beneficjent	Minister Cyfryzacji		
Partnerzy	NASK PIB		
Źródło finansowania	FUNDUSZE EUROPEJSKIE NA ROZWÓJ CYFROWY 2021-2027 (FERC) Priorytet IV - Wzmocnienie cyberbezpieczeństwa oraz rozwój odpornej infrastruktury przetwarzania danych; działanie 4.1 Wzmocnienie cyberbezpieczeństwa oraz rozwój odpornej infrastruktury przetwarzania danych; Środki zaplanowane są w budżecie dysponenta w części 27		
Całkowity koszt przedsięwzięcia	120 000 000,00 zł		
Planowany okres realizacji przedsięwzięcia	01-2027 do 06-2030		
Osoba kontaktowa	Artur Raciborski	artur.raciborski@nask.pl	786826027

1. POWODY PODJĘCIA PRZEDSIĘWZIĘCIA

1.1. Identyfikacja problemu i potrzeb

Bezpieczna komunikacja w administracji publicznej to fundament suwerenności cyfrowej państwa. W polskim porządku prawnym i strategicznym zagadnienie to ewoluowało od prostej ochrony poczty elektronicznej do budowy kompleksowych, izolowanych systemów wymiany informacji.
Istotę tego zagadnienia podkreśla szereg dokumentów o charakterze strategicznym i prawnym, które wymieniono poniżej:
1. W Strategii Cyberbezpieczeństwa RP wskazano, potrzebę rozbudowy systemów bezpiecznej komunikacji; ”Systemy bezpiecznej wymiany informacji na potrzeby kierowania bezpieczeństwem narodowym są konieczne nie tylko dla zapewnienia cyberbezpieczeństwa w kraju, ale także dla kompleksowego systemu bezpieczeństwa narodowego.". W obszarze interwencji 1.3 wprost wskazano na konieczność budowy SBŁP (Systemu Bezpiecznej Łączności Państwowej) i kontynuowania prac nad systemami wchodzącymi w skład ekosystemu SKR-Z: w obszarze niejawnym i jawnym ("komunikator").
problem: niewystarczający dostęp do kanałów bezpiecznej komunikacji
potrzeba: rozbudowa SKR-Z pod kątem liczby użytkowników i nowych funkcjonalności
2. W nowelizacji Ustawy o Krajowym Systemie Cyberbezpieczeństwa dostrzeżono konieczność zapewnienia kanałów komunikacji na potrzeby krajowego systemu cyberbezpieczeństwa. W związku z powyższym do wykazu podmiotów kluczowych i ważnych art 7 ust 2 pkt 11) wprowadzane są dane osób do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa. Co więcej w art 8. ust 1 pkt 2) lit. l) nałożono na podmioty kluczowe lub podmioty ważne wymóg stosowania bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa oraz wewnątrz podmiotu.
problem: brak jednolitego kanału bezpiecznej komunikacji dla wszystkich podmiotów KSC
Potrzeba: zapewnienie bezpiecznego kanału komunikacji, w tym komunikacji audio/video dla podmiotów KSC.

Odwołanie: art 8 ust 1 pkt 2) lit. l) w powiązaniu z Art. 7 ust 1 pkt 11) oraz art 45 ust 1. 9) Ustawy o KSC;
Cytat: powyżej.

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
Minister Cyfryzacji	* Zidentyfikowany problem: Niewystarczające mechanizmy komunikacyjne na potrzeby wykrywania kryzysów w cyberbezpieczeństwie; sytuacja w której występuje problem: sytuacja kryzysowa w cyberbezpieczeństwie; skutek: problemy ze skomunikowaniem się z osobami kontaktowymi; komunikacja przy pomocy kanałów niezapewniających poufności informacji, brak obrazu sytuacyjnego związanego z usuwaniem skutków sytuacji kryzysowej;	1
Podmioty krajowego systemu cyberbezpieczeństwa niekorzystające z części jawnej SKR (SKR-J)	* Zidentyfikowany problem: ograniczony dostęp do narzędzi do komunikacji mobilnej; sytuacja w której występuje problem: konieczność bezpiecznej komunikacji w trybie interaktywnym z innym podmiotem; skutek: możliwość podszycia się pod przedstawicieli innych instytucji (np. przy wykorzystaniu narzędzi AI), ze względu na brak pewności, że komunikacja jest prowadzona z uwierzytelnioną stroną przez bezpieczny kanał komunikacji. * Zidentyfikowany problem: brak usług umożliwiających wizualizację obrazu sytuacyjnego na urządzeniach mobilnych służących do komunikacji operacyjnej; sytuacja w której występuje problem: sytuacja kryzysowa; skutek: utrudnienia w koordynacji działań mitygujących skutki sytuacji kryzysowej, trudności w rozpoznaniu aktualnego przebiegu działań naprawczych, lub sytuacji kryzysowej;	37 000
Podmioty krajowego systemu cyberbezpieczeństwa korzystające z części jawnej SKR (SKR-J)	* Zidentyfikowany problem: ograniczone możliwości bezpiecznej komunikacji w obszarze komunikacji jawnej; sytuacja, w której występuje problem: konieczność bezpiecznej komunikacji w trybie interaktywnym z podmiotem niekorzystającym z SKR-J. Skutek: możliwość podszycia się pod przedstawicieli innych instytucji (np. przy wykorzystaniu narzędzi AI), ze względu na brak pewności, że komunikacja jest prowadzona z uwierzytelnioną stroną przez bezpieczny kanał komunikacji. * Zidentyfikowany problem: brak narzędzi umożliwiających wizualizację obrazu	1000

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
	sytuacyjnego na urządzeniach mobilnych i w trakcie działań operacyjnych.; sytuacja, w której występuje problem: sytuacja kryzysowa; skutek: utrudnienia w koordynacji działań mitygujących skutki sytuacji kryzysowej, trudności w rozpoznaniu aktualnego przebiegu działań naprawczych, lub sytuacji kryzysowej;	
Podmioty publiczne, podmioty KSC i inne podmioty posiadające potrzebę tworzenia dokumentów o klauzuli "zastrzeżone" - niepodłączone do części niejawnej SKR (SKR-N)	* Zidentyfikowany problem: brak możliwości szybkiego i bezpiecznego przekazywania informacji niejawnych o klauzuli "zastrzeżone" do innych podmiotów; sytuacja: przekazanie dokumentów niejawnych; skutek: konieczność przesyłania dokumentów w formie papierowej, kurierem, albo przekazywania informacji na spotkaniu bezpośrednim; opóźnienia w komunikacji; dodatkowe koszty; * Zidentyfikowany problem: brak możliwości współdzielenia i podglądu na urządzeniach mobilnych obrazu sytuacyjnego uwzględniającego informacje o charakterze niejawnym; sytuacja, w której występuje problem: sytuacje kryzysowe; skutek: utrudnienia w koordynacji działań mitygujących skutki sytuacji kryzysowej, trudności w rozpoznaniu aktualnego przebiegu działań naprawczych, lub sytuacji kryzysowej	13000
Podmioty publiczne, podmioty KSC i inne podmioty posiadające potrzebę tworzenia dokumentów o klauzuli "zastrzeżone" - podłączone do części niejawnej SKR (SKR-N)	* Zidentyfikowany problem: ograniczony obszar szybkiego i bezpiecznego przekazywania informacji niejawnych o klauzuli "zastrzeżone" do innych podmiotów; sytuacja, w której występuje problem: przekazanie dokumentów i informacji o klauzuli „zastrzeżone” do podmiotów niepodłączonych do SKR-Z; skutek: konieczność przesyłania dokumentów w formie papierowej, kurierem, albo przekazywania informacji na spotkaniu bezpośrednim; opóźnienia w komunikacji; dodatkowe koszty; * Zidentyfikowany problem: brak możliwości współdzielenia i podglądu na urządzeniach mobilnych obrazu sytuacyjnego uwzględniającego informacje o charakterze niejawnym; sytuacja, w której występuje problem: sytuacje kryzysowe; skutek: utrudnienia w koordynacji działań mitygujących skutki sytuacji kryzysowej, trudności w rozpoznaniu aktualnego	700

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
	przebiegu działań naprawczych, lub sytuacji kryzysowej	

1.2. Opis stanu obecnego

Aktualnie, system SKR-Z udostępnia usługi bezpiecznej komunikacji takie jak mail, komunikator w części jawnej i niejawnej. Podłączanie do części niejawnej wymaga dedykowanych urządzeń końcowych (laptop, telefon). Wąskim gardłem związanym z podłączaniem do systemu jest skalowalność rozwiązania oraz niska przepustowość procesów podłączania do systemu. Dotychczasowe procesy opierają się na manualnym przesyłaniu dokumentów niezbędnych do podłączenia do systemu. Ze względu na ograniczenia związane z dostępem do części niejawnej systemu, proces wnioskowania jest szczególnie trudny.
Optymalizacja procesu podłaczania wraz z opracowaniem usługi umożliwiającej automatyzację wnioskowania o dostęp do systemu pozwoli odblokować "wąskie gardło" i zwiększyć ilość podłaczanych podmiotów zarówno w części jawnej jak i niejawnej systemu.
System SKR-Z nie posiada aktualnie narzędzi umożliwiających współdzielenie obrazu sytuacyjnego. Jest to kłopotliwe szczególnie w części niejawnej, gdzie nie jest możliwe stosowanie rozwiazań zastępczych. Taka sytuacja utrudnia postrzeganie aktualnego stanu sytuacji, szczególnie w przypadkach kryzysowych. Wprowadzenie dedykowanych narzędzi, dostępnych dla podmiotów podłączonych do systemu SKR-Z powinno znieść wyżej wymienioną niedogodność i podnieść jakość współpracy w sytuacjach kryzysowych.
Udostępnianie technologii nowym użytkownikom, zawsze jest powiązane z koniecznością ich przeszkolenia z wykorzystania tych technologii. Z tego względu zaplanowano również stosowne szkolenia dla nowych użytkowników.
Dynamiczne zwiększenie liczby użytkowników wiąże się z koniecznością rozbudowy pojemności systemu, tak aby zapewnić nieprzerwaną pracę systemu oraz stosowną redundancję.
Podłaczenie do części niejawnej systemu wymaga również stosowania dedykowanych urządzeń końcowych, których zakup jest niezbędny w przypadku podłączania nowych użytkowników części niejawnej. W ramach projektu przewidziano środki na zakup wyżej wymienionych urządzeń.

2. EFEKTY PRZEDSIĘWZIĘCIA

W jaki sposób przedsięwzięcie realizuje Strategię Cyfryzacji Państwa?	Niniejszy projekt wpisuje się w zakres strategii cyfryzacji państwa, a w szczególności w realizację celu 1.3.3: systemy informacyjne w sferze publicznej (w tym militarnej) oraz prywatnej posiadają wysoki poziom odporności. W pkt a) wskazano konieczność "kontynuacji już realizowanych inicjatyw w obszarze [...] bezpiecznej łączności". Niniejszy projekt, ma na celu rozbudowę i rozwój istniejącego przedsięwzięcia w obszarze bezpiecznej komunikacji. W pkt. h) wskazano, że konieczne jest "umożliwienie przetwarzania informacji niejawnych w rządowych narzędziach chmurowych oraz zdefiniowanie w przepisach prawa zasad i wymagań dotyczących przetwarzania informacji niejawnych w chmurze obliczeniow ej, w tym zasad

	przyznawania, odbierania i monitorowania dostępu". Niniejsze zagadnienie odnosi się w szczególności do usług komunikacyjnych udostępnianych w formie chmurowej w systemie SKR-Z, których rozbudowa jest przedmiotem niniejszego przedsięwzięcia.
Jakie inne strategie, polityki publiczne lub wymagania strategiczne realizuje przedsięwzięcie?	Strategia Cyberbezpieczeństwa RP cel szczegółowy 1: Rozwój krajowego systemu cyberbezpieczeństwa Obszar interwencji 1.3: Rozwój zintegrowanego systemu wymiany informacji na potrzeby zapewnienia ciągłosci funkcjonowania administracji państwowej bezpieczeństwa narodowego i ochrony ludności Zakres; wprost wskazano na konieczność budowy SBŁP (Systemu Bezpiecznej Łączności Państwowej) i kontynuowania prac nad systemami wchodzącymi w skład ekosystemu SKR-Z: w obszarze niejawnym i jawnym ("komunikator")

2.1. Cele i korzyści wynikające z przedsięwzięcia

Cel - 1	Upowszechnienie narzędzi do bezpiecznej komunikacji w obszarze jawnym
Cel strategiczny	Strategia Cyberbezpieczeństwa RP cel szczegółowy 1: Rozwój krajowego systemu cyberbezpieczeństwa Obszar interwencji 1.3: Rozwój zintegrowanego systemu wymiany informacji na potrzeby zapewnienia ciągłosci funkcjonowania administracji państwowej bezpieczeństwa narodowego i ochrony ludności Zakres; wprost wskazano na konieczność budowy SBŁP (Systemu Bezpiecznej Łączności Państwowej) i kontynuowania prac nad systemami wchodzącymi w skład ekosystemu SKR-Z: w obszarze niejawnym i jawnym ("komunikator")
Korzyść:	* zwiększenie poziomu bezpieczeństwa podczas wymiany informacji pomiędzy podmiotami poprzez zastosowanie sprawdzonych narzędzi * rezygnacja z narzędzi komercyjnych (Signal, WhatsApp) do przekazywania informacji wrażliwych na rzecz narzędzi bezpiecznej komunikacji wytworzonych w projekcie * usprawnienie kontaktów między instytucjami KSC poprzez zastosowanie wspólnego katalogu użytkowników i wspólnej platformy wymiany informacji * zapewnienie elastyczności w zarządzaniu użytkownikami poprzez mechanizmy delegacji narzędzi do komunikacji w części jawnej * usprawnienie onboardingu instytucji poprzez integrację z usługami ekosystemu S46 w celu zakładania instytucji
KPI:	KPI1: Liczba zoptymalizowanych procesów podłączenia do części jawnej systemu SKR-Z (SKR-J) KPI2: Liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym (sumarycznie) KPI3: Liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym (kobiety) KPI4: Liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym (mężczyźni) KPI5: Liczba pracowników podmiotów wykonujących zadania publiczne niebędących pracownikami IT, objętych wsparciem szkoleniowym

	(sumarycznie) KPI6: Liczba pracowników podmiotów wykonujących zadania publiczne niebędących pracownikami IT, objętych wsparciem szkoleniowym (kobiety) KPI7: Liczba pracowników podmiotów wykonujących zadania publiczne niebędących pracownikami IT, objętych wsparciem szkoleniowym (mężczyźni) KPI8: Instytucje publiczne otrzymujące wsparcie na opracowywanie usług, produktów i procesów cyfrowych – 1 MC; KPI9: Liczba podmiotów wspartych w zakresie rozwoju usług, produktów i procesów cyfrowych – 1 (NASK PIB); KPI10: Przepustowość procesu podłączania w obszarze jawnym (podłączone instytucje/mies); KPI11: Skrócenie czasu realizacji procesu podłączenia podmiotu do SKR-Z end-to-end;
Wartość aktualna i docelowa KPI:	KPI1: - wartość aktualna: 0 KPI2: - wartość aktualna: 0 KPI3: - wartość aktualna: 0 KPI4: - wartość aktualna: 0 KPI5: - wartość aktualna: 0 KPI6: - wartość aktualna: 0 KPI7: - wartość aktualna: 0 KPI8: - wartość aktualna: 0 KPI9: - wartość aktualna: 0 KPI10: - wartość aktualna: 16 KPI11: - wartość aktualna: czas - ustalony wg stanu przed wdrożeniem rozwiązania KPI1: - wartość docelowa: 1 KPI2: - wartość docelowa: 1300 KPI3: - wartość docelowa: 240 KPI4: - wartość docelowa: 1060 KPI5: - wartość docelowa: 1300 KPI6: - wartość docelowa: 240 KPI7: - wartość docelowa: 1060 KPI8: - wartość docelowa: 1 KPI9: - wartość docelowa: 1

	KPI10: - wartość docelowa: 32 KPI11: - wartość docelowa: -10%
Metoda pomiaru KPI	KPI1: Metoda pomiaru: Badanie ewaluacyjne ilościowe; Źródło danych: Raport z wdrożenia zoptymalizowanego procesu podłączenia do części jawnej (SKR-J); częstotliwość pomiaru: rok po zakończeniu realizacji projektu KPI2: Metoda Pomiaru: Badanie ewaluacyjne ilościowe; źródło danych: podpisane przez prowadzącego listy obecności na szkoleniach zdalnych lub stacjonarnych; częstotliwość pomiaru; na koniec każdego roku realizacji projektu; ostatni pomiar na koniec realizacji projektu. KPI3: Metoda Pomiaru: Badanie ewaluacyjne ilościowe; źródło danych: podpisane przez prowadzącego listy obecności na szkoleniach zdalnych lub stacjonarnych; częstotliwość pomiaru; na koniec każdego roku realizacji projektu; ostatni pomiar na koniec realizacji projektu. KPI4: Metoda Pomiaru: Badanie ewaluacyjne ilościowe; źródło danych: podpisane przez prowadzącego listy obecności na szkoleniach zdalnych lub stacjonarnych; częstotliwość pomiaru; na koniec każdego roku realizacji projektu; ostatni pomiar na koniec realizacji projektu. KPI5: Metoda Pomiaru: Badanie ewaluacyjne ilościowe; źródło danych: podpisane przez prowadzącego listy obecności na szkoleniach zdalnych lub stacjonarnych; częstotliwość pomiaru; na koniec każdego roku realizacji projektu; ostatni pomiar na koniec realizacji projektu. KPI6: Metoda Pomiaru: Badanie ewaluacyjne ilościowe; źródło danych: podpisane przez prowadzącego listy obecności na szkoleniach zdalnych lub stacjonarnych; częstotliwość pomiaru; na koniec każdego roku realizacji projektu; ostatni pomiar na koniec realizacji projektu. KPI7: Metoda Pomiaru: Badanie ewaluacyjne ilościowe; źródło danych: podpisane przez prowadzącego listy obecności na szkoleniach zdalnych lub stacjonarnych; częstotliwość pomiaru; na koniec każdego roku realizacji projektu; ostatni pomiar na koniec realizacji projektu. KPI8: Metoda pomiaru: monitoring danych ilościowych przez biuro projektu; źródło danych: rozliczona umowa o dofinansowanie; częstotliwość pomiaru: na koniec realizacji projektu; KPI9: Metoda pomiaru: monitoring danych ilościowych przez biuro projektu; źródło danych: przyjęty raport z rozliczenia projektu; częstotliwość pomiaru: na koniec realizacji projektu; KPI10: Metoda pomiaru: Badanie ewaluacyjne ilościowe; Źródło danych: liczba nowych instytucji podłączonych do części jawnej w ciągu miesiąca; za wartość wskaźnika przyjmowana jest maksymalna liczba spośród wszystkich miesięcy w okresie trwania projektu; częstotliwość pomiaru: na koniec każdego roku realizacji projektu; ostatni pomiar na koniec realizacji projektu; KPI11: Metoda pomiaru: porównanie mediany czasu realizacji procesu podłączenia podmiotu przed wdrożeniem i po wdrożeniu zoptymalizowanego procesu. Czas realizacji procesu end-to-end liczony jest od dnia przyjęcia kompletnego zgłoszenia podmiotu do dnia uzyskania przez użytkownika możliwości korzystania z właściwej części SKR-Z. Pomiar będzie prowadzony odrębnie dla części jawnej i niejawnej ze względu na różnice w przebiegu procesów, wymaganiach formalnych oraz wymaganiach bezpieczeństwa. Źródło danych: rejestr zgłoszeń dotyczących podłączenia do SKR-Z oraz potwierdzenia uruchomienia dostępu do właściwej części systemu.

	Częstotliwość pomiaru: wartość bazowa przed uruchomieniem zoptymalizowanego procesu, następnie raz w roku oraz na zakończenie realizacji projektu.
Cel - 2	Upowszechnienie narzędzi do bezpiecznej komunikacji w obszarze niejawnym
Cel strategiczny	Strategia Cyberbezpieczeństwa RP cel szczegółowy 1: Rozwój krajowego systemu cyberbezpieczeństwa Obszar interwencji 1.3: Rozwój zintegrowanego systemu wymiany informacji na potrzeby zapewnienia ciągłości funkcjonowania adminstracji państwowej bezpieczeństwa narodowego i ochrony ludności Zakres; wprost wskazano na konieczność budowy SBŁP (Systemu Bezpiecznej Łączności Państwowej) i kontynuowania prac nad systemami wchodzącymi w skład ekosystemu SKR-Z: w obszarze niejawnym i jawnym ("komunikator")
Korzyść:	* Zapewnienie bezpiecznej łączności umożliwiającej wymianę informacji niejawnych na poziomie "zastrzeżone/EU RESTRAINT/NATO RESTRICTED" * zwiększenie wykorzystania cyfrowej wymiany informacji w obszarze niejawnym, * ułatwienie współpracy nad wytwarzaniem dokumentów niejawnych w obrębie pojedynczej instytucji oraz w obrębie wielu instytucji; * zmniejszenie liczby spotkań osobistych wymagających wymiany informacji niejawnych ze względu na udostępnienie narzędzi do komunikacji grupowej.
KPI:	KPI12: Liczba zoptymalizowanych procesów podłączenia do części niejawnej systemu SKR-Z (SKR-N) KPI13: Liczba podmiotów wspartych w zakresie cyberbezpieczeństwa; KPI14: Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych; KPI15: Przepustowość podłączania w obszarze niejawnym (liczba instytucji/ mies);
Wartość aktualna i docelowa KPI:	KPI12: - wartość aktualna: 0 KPI13: - wartość aktualna: 0 KPI14: - wartość aktualna: 0 KPI15: - wartość aktualna: 55 KPI12: - wartość docelowa: 1 KPI13: - wartość docelowa: 1000 KPI14: - wartość docelowa: 2600 KPI15: - wartość docelowa: 75
Metoda pomiaru KPI	KPI12: Metoda pomiaru: Badanie ewaluacyjne ilościowe; Źródło danych: Raport z wdrożenia zoptymalizowanego procesu podłączenia do części niejawnej (SKR-N); częstotliwość pomiaru: rok po zakończeniu realizacji projektu KPI13: Metoda pomiaru: Badanie ewaluacyjne ilościowe; Źródło danych: Lista podmiotów podłączonych do systemu w raportowanym okresie (narastająco) (SKR-N); częstotliwość pomiaru: na koniec każdego roku realizacji projektu.

	ostatni pomiar na koniec realizacji projektu. KPI14: Metoda pomiaru: Badanie ewaluacyjne ilościowe; Źródło danych: Lista użytkowników podłączonych do systemu w raportowanym okresie (narastająco) (SKR-N); częstotliwość pomiaru: na koniec każdego roku realizacji projektu KPI15: Metoda pomiaru: Badanie ewaluacyjne ilościowe; Źródło danych: liczba nowych użytkowników podłączonych do części jawnej w ciągu miesiąca; za wartość wskaźnika przyjmowana jest maksymalna liczba spośród wszystkich miesięcy w okresie trwania projektu; częstotliwość pomiaru: na koniec każdego roku realizacji projektu; ostatni pomiar na koniec realizacji projektu;
Cel - 3	Udostępnienie systemu do współdzielenia obrazu sytuacyjnego w obszarze Jawnym oraz w obszarze niejawnym
Cel strategiczny	Strategia Cyberbezpieczeństwa RP cel szczegółowy 1: Rozwój krajowego systemu cyberbezpieczeństwa Obszar interwencji 1.3: Rozwój zintegrowanego systemu wymiany informacji na potrzeby zapewnienia ciągłości funkcjonowania adminstracji państwowej bezpieczeństwa narodowego i ochrony ludności Zakres; wprost wskazano na konieczność kontynuowania prac nad systemami wchodzącymi w skład ekosystemu SKR-Z: w obszarze niejawnym i jawnym ("komunikator") [...] w zakresie nowych funkcjonalności.
Korzyść:	* zwiększenie możliwości wymiany informacji i reagowania na sytuacje kryzysowe poprzez zapewnienie i współdzielenie obrazu sytuacyjnego * podniesienie możliwości współpracy w przypadku sytuacji kryzysowych, pomiędzy instytucjami podłączonymi do systemu w części jawnej * podniesienie możliwości współpracy w przypadku sytuacji kryzysowych, pomiędzy instytucjami podłączonymi do systemu w części niejawnej * Zapewnienie kopmatybilności kanałów wymiany informacji z jednostkami wykorzystującymi systemy w obszarze wojskowym
KPI:	KPI16: Liczba zmodernizowanych systemów
Wartość aktualna i docelowa KPI:	KPI15: - wartość aktualna: 0 KPI15: - wartość docelowa: 1
Metoda pomiaru KPI	KPI15: Metoda pomiaru: Badanie ewaluacyjne ilościowe: Źródło danych: Raport z wdrożenia zoptymalizowanego systemu; częstotliwość pomiaru: ostatni dzień realizacji projektu;

2.2. Udostępnione e-usługi

Lp.	Nazwa e-usługi	Typ	Zakres oddziaływania	Poziom dojrzałosci e-usługi
1	wnioskowanie o dołączenie do systemu SKR-Z	A2A A2B	Podmioty krajowego systemu cyberbezpieczeństwa niekorzystające z części jawnej SKR (SKR-J) Podmioty publiczne,	Transakcja

Lp.	Nazwa e-usługi	Typ	Zakres oddziaływania	Poziom dojrzałosci e-usługi
			podmioty KSC i inne podmioty posiadające potrzebę tworzenia dokumentów o klauzuli "zastrzeżone" - niepodłączone do części niejawnej SKR (SKR-N) (rocznie ok 1000 transakcji)	

2.3. Udostępnione informacje sektora publicznego i zdigitalizowane zasoby

Nie dotyczy

2.4. Produkty końcowe przedsięwzięcia

Nazwa produktu	Planowana data wdrożenia
Raport z inicjalnego testu prywatności	01-2027
Koncepcja usprawnienia procesu podłączania użytkowników w środowisku jawnym (SKR-J)	03-2027
Koncepcja usprawnienia procesu podłaczenia użytkowników w środowisku niejawnym (SKR-N)	03-2027
Materiały szkoleniowe dotyczące usług komunikacji	03-2027
Raport z weryfikacyjnego testu prywatności	09-2027
raport z testów bezpieczeństwa, wydajności UX/UI oraz WCAG usługi wnioskowania o dołączenie do SKR-Z	10-2027
Dokumentacja akredytacyjna zaktualizowana o część niejawną usługi wnioskowania do SKR-Z	12-2027
Koncepcja wdrożenia Współdzielenia obrazu sytuacyjnego w środowisku jawnym	09-2027
Współdzielenie obrazu sytuacyjnego - POC	03-2028
Współdzielenie obrazu sytuacyjnego w środowisku jawnym	06-2028
Koncepcja współdzielenia obrazu sytuacyjnego w środowisku niejawnym	03-2029
Współdzielenie obrazu sytuacyjnego w środowisku niejawnym	12-2029
Dokumentacja systemu zaktualizowanego o obszar współdzielenia obrazu sytuacyjnego w środowisku niejawnym	12-2029
Zmodyfikowany system SKR-Z	12-2029
Rozbudowana infrastruktura teleinformatyczna SKR-Z	12-2029

Nazwa produktu	Planowana data wdrożenia
Pozytywny raport z testów wydajności zmodyfikowanego systemu SKR-Z	12-2029
Raport z badań i testów UX zmodyfikowanego systemu SKR-Z	12-2029
Materiały informacyjno-promocyjne projektu	06-2030
Raport z wdrożenia zmodyfikowanego systemu	06-2030

3. KAMIENIE MILOWE

Kamienie milowe	Planowany termin osiągnięcia
Zatwierdzono docelowy model procesów podłączania do części jawnej i niejawnej SKR-Z	2027-06-30
Uruchomiono zoptymalizowany proces wnioskowania i podłączania do SKR-Z	2027-12-31
Potwierdzono wykonalność rozwiązania współdzielenia obrazu sytuacyjnego w środowisku jawnym	2028-03-31
Uruchomiono współdzielenie obrazu sytuacyjnego w środowisku jawnym	2028-06-30
Zatwierdzono docelową koncepcję współdzielenia obrazu sytuacyjnego w środowisku niejawnym	2029-03-31
Osiągnięto gotowość infrastruktury do obsługi docelowej skali SKR-Z	2029-09-30
Uruchomiono współdzielenie obrazu sytuacyjnego w środowisku niejawnym	2029-12-31
Uzyskano pozytywny wynik testów bezpieczeństwa	2029-12-31
Uzyskano pozytywny wynik testów wydajności	2029-12-31
Uzyskano pozytywny wynik badań i testów UX	2029-12-31
Zmodyfikowany system SKR-Z osiągnął gotowość produkcyjną	2030-03-31
Zakończono wdrożenie i potwierdzono osiągnięcie rezultatów projektu	2030-06-30

4. KOSZTY

4.1. Koszty ogólne przedsięwzięcia wraz ze sposobem finansowania

Całkowity koszt przedsięwzięcia (netto oraz brutto), w tym	Netto 87 446 621,38 zł Brutto 120 000 000,00 zł	
Procent dofinansowania ze środków UE (brutto)	89,93%	
Procent dofinansowania ze środków z innych źródeł zagranicznych (brutto)		
Procent środków z budżetu państwa (brutto)	10,07%	
Podział całkowitego kosztu przedsięwzięcia na poszczególne lata (netto oraz brutto)	2027	Netto 25 133 875,94 zł Brutto 34 483 809,38 zł
	2028	Netto 31 166 172,02 zł Brutto 42 682 577,60 zł
	2029	Netto 31 110 176,49 zł Brutto 42 779 938,15 zł
	2030	Netto 36 396,93 zł Brutto 53 674,87 zł

4.2. Wykaz poszczególnych pozycji kosztowych

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
Oprogramowanie	Do kategorii oprogramowanie zaliczono: zamawiane licencje, z wyłączeniem licencji dedykowanych do zapewnienia bezpieczeństwa, które zostały wliczone do pozycji "bezpieczeństwo", oraz koszty wytwarzania oprogramowania. Pozycje kosztowe powiązane z	34 827 433,61 zł	Zakup licencji (m.in. dostępowych) jest niezbędny do dystrybucji użytkownikom urządzeń końcowych w środowisku niejawnym. Planowany jest również zakup licencji do wirtualizacji, które są niezbędne do rozbudowy środowisk. Wytwarzanie oprogramowania wiąże się zarówno z pracami związanymi z usługami komunikacji, jak również z pracami związanymi z wytwarzaniem nowych usług, czy obsługą błędów i korektami dla istniejących usług. W zakres kosztu wliczono również koszt linii wsparcia

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
	produktami: Koncepcja usprawnienia procesu podłączania użytkowników w środowisku jawnym (SKR-J); Koncepcja usprawnienia procesu podłączenia użytkowników w środowisku niejawnym (SKR-N); Dokumentacja akredytacyjna zaktualizowana o część niejawną usługi wnioskowania do SKR-Z; Koncepcja wdrożenia Współdzielenia obrazu sytuacyjnego w środowisku jawnym; Współdzielenie obrazu sytuacyjnego - POC; Współdzielenie obrazu sytuacyjnego w środowisku jawnym; Koncepcja współdzielenia obrazu sytuacyjnego w środowisku niejawnym; Współdzielenie obrazu sytuacyjnego w środowisku niejawnym; Dokumentacja systemu zaktualizowanego o obszar		

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
	współdzielenia obrazu sytuacyjnego w środowisku niejawnym; Zmodyfikowany system SKR-Z; Raport z wdrożenia zmodyfikowanego systemu;		
Infrastruktura	Do kategorii infrastruktura wliczono zakupy dotyczące części infrastrukturalnej - serwerowej dla nowych usług: sprzęt, usługi, zakupy niskocenne, jak również urządzenia końcowe i niezbędne usługi wsparcia. Pozycje kosztowe powiązane w następującymi produktami: Rozbudowana infrastruktura teleinformatyczna SKR-Z; Zmodyfikowany system SKR-Z; Raport z wdrożenia zmodyfikowanego systemu.	57 255 860,12 zł	Zakupy związane z rozbudową infrastruktury na potrzeby nowych usług: serwery, urządzenia sieciowe, materiały takie jak wkładki, kable inne materiały niezbędne do montażu i użytkowania serwerów, urządzenia końcowe telefony i laptopy. Pozycja obejmuje również usługi związane z infrastrukturą takie jak kolokacja serwerowni, usługi połączeniowe, czy materiały niezbędne do uruchomienia nowej infrastruktury wsparcia i zapewnienia działania usług na potrzeby podłączeń.
Koszty UX i grafiki	Do kategorii wliczono: koszty personelu projektującego warstwę graficzną i zapewniającego wygodę użytkowania; Pozycja kosztowa powiązana bezpośrednio z produktami: raport z testów	1 203 732,00 zł	W ramach projektu przewidywane jest wytworzenie usług automatyzujących onboarding użytkowników oraz dostosowywanie usług komunikacji. Ze względu na wystawienie interfejsu dla użytkowników zewnętrznych, konieczne jest zapewnienie atrakcyjnej szaty graficznej oraz wygody użytkowania.

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
	bezpieczeństwa, wydajności UX/UI oraz WCAG usługi wnioskowania o dołączenie do SKR-Z; Raport z badań i testów UX zmodyfikowanego systemu SKR-Z		
Bezpieczeństwo	Do kategorii wliczono zakupy urządzeń i oprogramowania oraz usług niezbędnych do zapewnienia bezpieczeństwa. Rozbudowana infrastruktura teleinformatyczna SKR-Z; Zmodyfikowany system SKR-Z; Raport z wdrożenia zmodyfikowanego systemu; Raport z inicjalnego testu prywatności; Raport z weryfikacyjnego testu prywatności; raport z testów bezpieczeństwa, wydajności UX/UI oraz WCAG usługi wnioskowania o dołączenie do SKR-Z;	9 586 349,00 zł	w zakres pozycji kosztowej wchodzą zakupy związane z ochroną końcówek (m. in. specjalistyczne oprogramowanie do zarządzania oraz oprogramowanie do ochrony danych, oprogramowanie SIEM) oraz sprzętowe urządzenia związane z zapewnieniem bezpieczeństwa (np. tokeny do ochrony końcówek).
Wydajność rozwiązań	Do kategorii zaliczono głównie koszty osobowe. Pozycja kosztowa powiązana bezpośrednio z produktami: Zmodyfikowany system SKR-Z; Pozytywny raport z testów wydajności zmodyfikowanego	1 203 732,00 zł	W zakres zakupów wchodzą koszty osobowe związane z wdrożeniem rozwiązań zapewniających wzrost wydajności systemu. Zwiększenie wydajności jest wymagane w celu zapewnienia obsługi zwiększonej liczby użytkowników,

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
	systemu SKR-Z; raport z testów bezpieczeństwa, wydajności UX/UI oraz WCAG usługi wnioskowania o dołączenie do SKR-Z;		
Szkolenia	szkolenia użytkowników systemu i personelu projektowego. Pozycja kosztowa powiązana bezpośrednio z produktami; Materiały szkoleniowe dotyczące usług komunikacji;	687 913,82 zł	Zakup szkoleń specjalistycznych dla personelu wiąże się z koniecznością zapewnienia odpowiednich kompetencji w rozbudowywanych obszarach sytemu. Szkolenia dla użytkowników zewnętrznych są bezpośrednio powiązane ze wskaźnikami projektu. Przygotowanie materiałów szkoleniowych jest bezpośrednio związane z prowadzeniem szkoleń dla użytkowników zewnętrznych.
Działania informacyjno-promocyjne	zakupy tablic i organizacja konferencji; Pozycja kosztowa powiązana bezpośrednio z produktami: 18 Materiały informacyjno-promocyjne projektu	520 000,00 zł	Pozycja budżetowa wynika bezpośrednio z wymagań dotyczących wykorzystywania środków UE. W ramach pozycji zaplanowano zakup tablic informacyjnych. Organizacja konferencji tematycznych pozwoli na zachęcenie podmiotów do dołączania do systemu SKR-Z, co powinno przełożyć się na osiągnięcie wskaźników dotyczących ilości instytucji i użytkowników.
Koszty zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego)	Pozycja kosztowa została podzielona na dwa obszary: zarządzanie - powiązane z projektem oraz koszty ogólne projektu. Pozycja kosztowa powiązana bezpośrednio z produktami: Raport z wdrożenia zmodyfikowanego systemu;	14 714 979,45 zł	W ramach kosztów uwzględniono koszty personelu odpowiedzialnego za nadzór projektu po stronie beneficjenta i partnera. W zakres wchodzą również koszty ogólne.

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

Całkowity koszt utrzymania trwałości przedsięwzięcia (brutto)	145 438 481,61 zł		**Źródło finansowania**
Podział całkowitego kosztu utrzymania trwałości przedsięwzięcia na poszczególne lata (netto oraz brutto)	2030	24 013 266,62 zł (brutto) (19 784 877,06 zł netto)	krajowe środki publiczne - budżet państwa
	2031	25 204 695,10 zł (brutto) (20 766 612,91 zł netto)	krajowe środki publiczne - budżet państwa
	2032	29 781 616,65 zł (brutto) (24 501 436,89 zł netto)	krajowe środki publiczne - budżet państwa
	2033	32 529 837,92 zł (brutto) (26 750 200,14 zł netto)	krajowe środki publiczne - budżet państwa
	2034	33 909 065,32 zł (brutto) (27 886 682,10 zł netto)	krajowe środki publiczne - budżet państwa

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

- 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 przedsięwzięcia

Nazwa ryzyka	**Siła oddziaływania**	**Prawdopo-dobieństwo wystąpienia ryzyka**	**Sposób zarzadzania ryzykiem**
Brak wystarczających środków na realizację projektu	Duża	Niskie	Bieżące monitorowanie realizacji budżetu projektu, okresowa analiza wykonania planu finansowego oraz zgodności wydatków z harmonogramem rzeczowo-finansowym. W przypadku identyfikacji zagrożeń będą

Nazwa ryzyka	Siła oddziaływania	Prawdopo-dobieństwo wystąpienia ryzyka	Sposób zarzadzania ryzykiem
			podejmowane działania korygujące obejmujące aktualizację planu wydatków, priorytetyzację zadań oraz bieżący nadzór nad realizacją kluczowych produktów projektu.
Przekroczenie harmonogramu realizacji projektu	Średnia	Niskie	Zaangażowanie odpowiednich zasobów projektowych, monitorowanie harmonogramu realizacji projektu, monitorowanie ryzyk projektowych i wprowadzanie działań zapobiegawczych na wczesnym etapie.
Nieosiągnięcie wskaźników produktu i celu projektu	Średnia	Niskie	Bieżący monitoring i raportowanie prac, monitorowanie wskaźników, efektywne zarządzanie ryzykiem projektowym.
Opóźnienia w realizacji projektu wpływające z przedłużających się procedur zakupowych w PZP.	Średnia	Średnie	Rozpoczęcie procedur zakupowych z wyprzedzeniem. Skracanie realizacji wykonywania zamówienia poprzez stosowanie umów ramowych dla powtarzanych zakupów (np. urządzeń końcowych).
Brak skutecznej koordynacji działań projektowych	Średnia	Znikome	Regularne spotkania zespołu projektowego. Przypisanie zadań projektowych członkom zespołu z uwzględnieniem ich kompetencji i doświadczenia. Uregulowanie zasad współpracy.
Niespełnienie oczekiwanych, planowanych, funkcjonalności nowych usług	Średnia	Znikome	Monitorowanie potrzeb użytkowników i dostosowywanie produktów do potrzeb użytkowników.
Niedostępność wymaganych zasobów i kompetencji specjalistycznych	Duża	Niskie	Bieżące planowanie zapotrzebowania na zasoby i kompetencje, wczesne angażowanie specjalistów oraz monitorowanie ich dostępności. Zapewnienie zastępowalności kluczowych osób, przekazywanie i dokumentowanie wiedzy oraz, w razie potrzeby, pozyskanie wsparcia zewnętrznego lub odpowiednia zmiana kolejności realizacji zadań.
Opóźnienie lub ograniczenie wdrożenia części	Średnia	Niskie	Wczesna identyfikacja wymagań bezpieczeństwa i akredytacji oraz ich uwzględnienie w architekturze,

Nazwa ryzyka	Siła oddziaływania	Prawdopo-dobieństwo wystąpienia ryzyka	Sposób zarzadzania ryzykiem
niejawnej wskutek niespełnienia wymagań bezpieczeństwa i akredytacji.			harmonogramie i dokumentacji rozwiązania. Prowadzenie konsultacji z właściwymi komórkami i organami, okresowa weryfikacja zgodności oraz etapowanie prac w sposób umożliwiający usuwanie niezgodności przed uruchomieniem części niejawnej.

5.2. Ryzyka wpływające na utrzymanie efektów

Nazwa ryzyka	Siła oddziaływania	Prawdopo-dobieństwo wystąpienia ryzyka	Sposób zarzadzania ryzykiem
Brak wystarczających zasobów organizacyjnych, kadrowych lub finansowych do zapewnienia utrzymania i dalszego rozwoju produktów projektu po zakończeniu finansowania.	Duża	Niskie	Budżetowanie z wyprzedzeniem środków finansowych na utrzymanie rozwiazania.
Utrata kluczowych kompetencji niezbędnych do utrzymania i rozwijania produktów projektu wskutek rotacji pracowników lub ograniczonej dostępności specjalistów.	Średnia	Niskie	Przygotowywanie dokumentacji technicznej i gromadzenie wiedzy niezbędnej do onboardingu nowych pracowników. Zapewnianie zastępowalności dla ról niezbędnych do utrzymania systemu.
Rezygnacja z wykorzystywania systemu przez użytkowników	Duża	Niskie	Monitorowanie potrzeb użytkowników, dostosowywanie i rozwój systemu zgodnie z kierunkiem potrzeb zgłaszanych przez uzytkowników.
Utrata ciągłości działania lub	Duża	Znikome	Zapewnienie monitorowania dostępności, wykonywania kopii

Nazwa ryzyka	Siła oddziaływania	Prawdopo-dobieństwo wystąpienia ryzyka	Sposób zarzadzania ryzykiem
wymaganej dostępności systemu			zapasowych, redundancji kluczowych komponentów oraz procedur reagowania na awarie i odtwarzania działania systemu. Regularne testowanie zabezpieczeń ciągłości działania, aktualizowanie procedur oraz zapewnienie odpowiedniego wsparcia utrzymaniowego.
Utrata zgodności rozwiązania z wymaganiami bezpieczeństwa, technicznymi lub akredytacyjnymi	Duża	Znikome	Stałe monitorowanie zmian wymagań bezpieczeństwa, standardów technicznych i warunków akredytacyjnych. Prowadzenie okresowych przeglądów zgodności, audytów i testów bezpieczeństwa oraz terminowe wdrażanie aktualizacji i działań naprawczych. Utrzymywanie aktualnej dokumentacji oraz planowanie niezbędnych modernizacji rozwiązania.

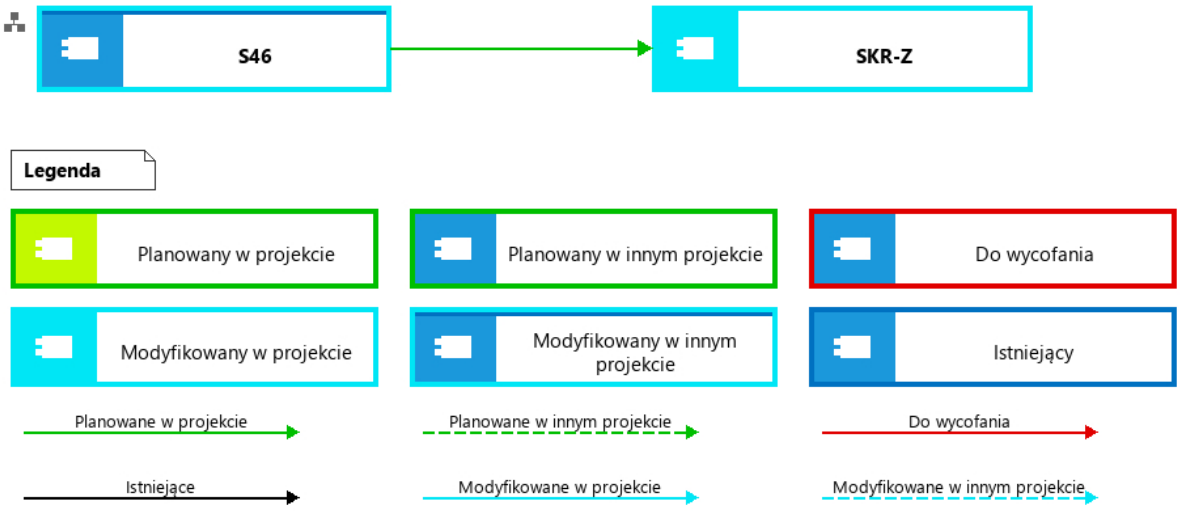
6. OTOCZENIE PRAWNE

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
1	Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych Dz.U 2010 nr 182 poz. 1228 późn. zm.	~~TAK~~/NIE		
2	Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa Dz. U. 2018 poz.1560 późn. zm.	~~TAK~~/NIE		
3	Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne z dnia 17 lutego 2005 r. (t.j. Dz.U. z 2024 r. poz. 1557)	~~TAK~~/NIE		
4	Ustawa o ochronie baz danych z dnia 27 lipca 2001 r. (t.j. Dz.U. z 2024 r. poz. 1769)	~~TAK~~/NIE		
5	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 z dnia 21	~~TAK~~/NIE		

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
	maja 2024 r. (Dz.U. z 2024 r. poz. 773)			
6	Ustawa o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych z dnia 4 kwietnia 2019 r. (t.j. Dz.U. z 2023 r. poz. 1440)	~~TAK~~/NIE		
7	Ustawa o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. (t.j. Dz.U. z 2024 r. poz. 1725)	~~TAK~~/NIE		
8	Rozporządzenie Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego z dnia 20 lipca 2011 r. (Dz.U. 2011 Nr 159, poz. 948)	~~TAK~~/NIE		
9	Ustawa o narodowym zasobie archiwalnym i archiwach z dnia 14 lipca 1983 r. (t.j. Dz.U. z 2020 r. poz. 164 ze zm. Dz. U. z 2021 poz. 398 i 2020)	~~TAK~~/NIE		
10	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)	~~TAK~~/NIE		
11	Ustawa o krajowym systemie cyberbezpieczeńsywa z dnia 5 lipca 2018 r. (Dz.U. 2018 poz. 1560 późn. zm.)	~~TAK~~/NIE		

7. ARCHITEKTURA

7.1. Widok kooperacji aplikacji



Lista systemów wykorzystywanych w przedsięwzięciu

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
1	SKR-Z	Ministerstwo Cyfryzacji	SKR-Z to system teleinformatyczny zapewniający wymianę informacji niejawnych z klauzulą „zastrzeżone”, przetwarzanych w administracji publicznej oraz zapewniający bezpieczne mechanizmy komunikacji do wymiany tych informacji i ograniczenie możliwości ich niepowołanego przejęcia. Celem systemu jest zapewnienie bezpiecznej komunikacji mobilnej w obszarze informacji niejawnych o klauzuli "zastrzeżone" oraz w obszarze komunikacji jawnej. Główne grupy	Istniejący	Usługi komunikacji niejawnej w SKR-Z (istniejący komponent) - modyfikacja w zakresie skalowania w związku ze zwiększoną liczbą użytkowników i korekty błędów rozwiązania; Usługi komunikacji jawnej w SKR-Z (istniejący komponent) - modyfikacja w zakresie

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			funkcjonalności: - usługi komunikacji niejawnej SKR-Z (audio/ video/ chat/mail); - zapewnienie możliwości tworzenia i edycji dokumentów o klauzuli zastrzeżone/NATO/UE restricted; - usługi komunikacji jawnej SKR-Z (audio/ video/chat); - wewnętrzne usługi identyfikacji i uwierzytelnienia dla części jawnej; - wewnętrzne usługi identyfikacji i uwierzytelnienia dla części niejawnej. System komunikuje się z innymi systemami teleinformatycznymi w obszarze niejawnym. Szczegóły komunikacji objęte klauzulą "zastrzeżone".		skalowania w związku ze zwiększoną liczbą użytkowników i korekty błędów rozwiązania; Aplikacja mobilna mSzyfr (istniejący komponent) - modyfikacja w zakresie obsługi zwiększonej liczby użytkowników i korektą błędów i zgłoszeń użytkowników; Wewnętrzne usługi identyfikacji i uwierzytelnienia dla części jawnej (istniejący komponent) - modyfikacja w zakresie automatyzacji tworzenia instytucji i inicjalnych użytkowników w związku z wdrożeniem usługi wnioskowania do dołączenie do SKR-Z; Wewnętrzne usługi identyfikacji i uwierzytelnienia dla części niejawnej

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
					(istniejący komponent) - modyfikacja w zakresie automatyzacji onboardingu użytkowników, w związku z wdrożeniem usługi wnioskowania do dołączenie do SKR-Z; Wnioskowanie o dołączenie do SKR-Z (nowy komponent) - utworzenie i udostępnienie usługi w zakresie integracji z S46 oraz obsługą zgłoszeń instytucji w części jawnej i w części niejawnej SKR-Z. Współdzielenie obrazu sytuacyjnego w obszarze jawnym (nowy komponent) - dostosowanie i udostępnienie funkcjonalnośc i Współdzielenie obrazu sytuacyjnego w obszarze niejawnym (nowy komponent) - dostosowanie

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
					i udostepnienie funkcjonalności ;.
2	S46	Ministerstwo Cyfryzacji	System S46 został uruchomiony przez ministra właściwego do spraw informatyzacji zgodnie z art. 46 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20, 252.). System wspierający realizację zadań krajowego systemu cyberbezpieczeństwa, określonych w art. 46 ust. 1 oraz ust. 1a ww. ustawy, w tym: 1) współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa; 2) generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa; 3) zgłaszanie i obsługę incydentów; 4) szacowanie ryzyka na poziomie krajowym; 5) ostrzeganie o cyberzagrożeniach; 6) czynności nadzorcze organów właściwych do spraw cyberbezpieczeństwa; 7) dokonywanie zgłoszenia naruszenia ochrony danych osobowych, o którym mowa w art. 33 rozporządzenia 2016/679 i art. 44 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w	Istniejący	

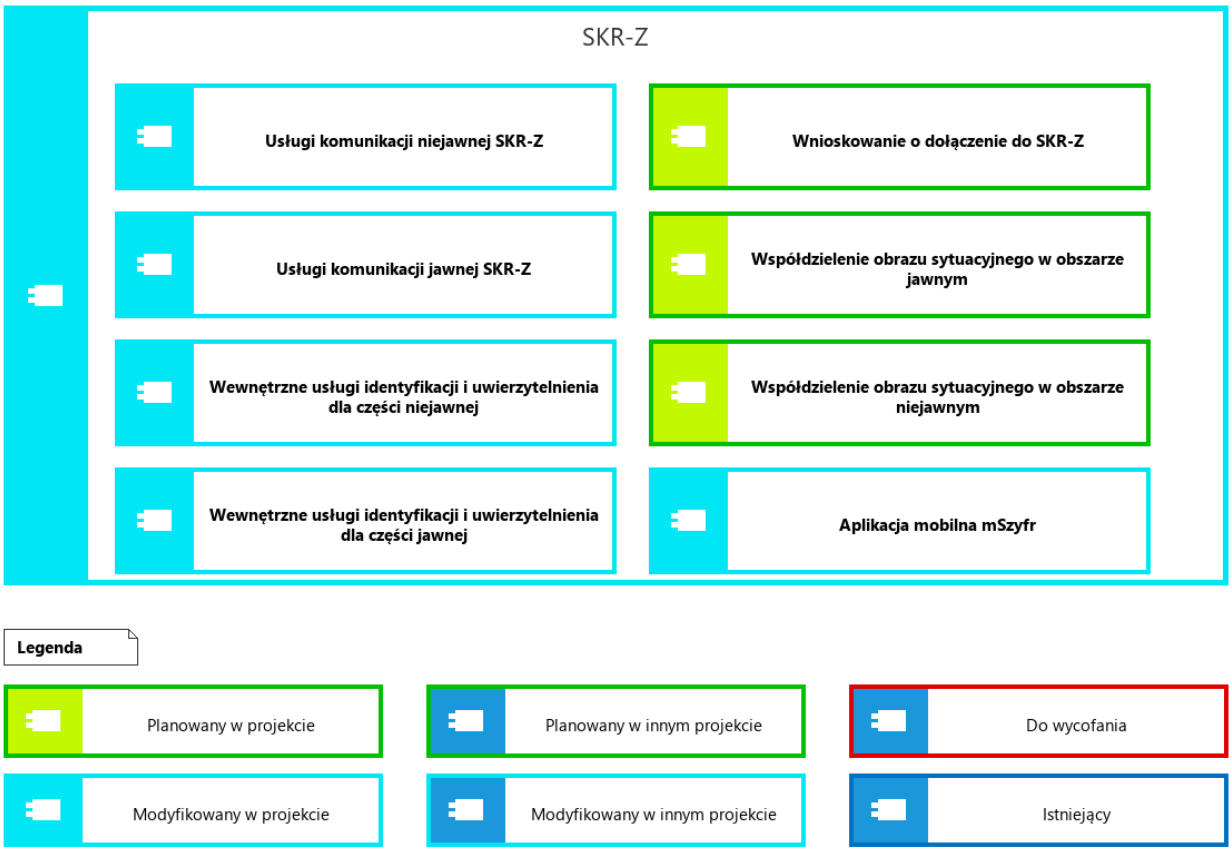
Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2023 r. poz. 1206), przez podmioty kluczowe lub podmioty ważne; 8) wymianę informacji o aktach ministra właściwego do spraw informatyzacji, Pełnomocnika, organów właściwych do spraw cyberbezpieczeństwa oraz Prezesa Rady Ministrów, o których mowa w art. 33 ust. 4, art. 42 ust. 1 pkt 5, art. 45 ust. 3, art. 67, art. 67a, art. 67b ust. 15, art. 67g ust. 1 i art. 67l ust. 1. 1a. W systemie teleinformatycznym prowadzi się wykaz* (*- Wykaz podmiotów kluczowych i podmiotów ważnych) Celem systemu jest zapewnienie obsługi incydentów, wymiany informacji oraz koordynacji działań. W systemie prowadzony jest rejestr publiczny – wykaz podmiotów kluczowych i ważnych. Główne funkcjonalności: • obsługa incydentów, • wymiana informacji między podmiotami, • zarządzanie ryzykiem, • ostrzeganie o zagrożeniach, • wsparcie procesów nadzorczych, • prowadzenie wykazu podmiotów. Integracje: System integruje się z licznymi systemami krajowymi i		

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			zagranicznymi, m.in. e-Doręczenia, moje.cert.pl, n6, NVD, Profil Zaufany.		

Lista przepływów

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
1	S46	SKR-Z	Informacje o instytucjach w wykazie podmiotów kluczowych i waznych oraz osobach wskazanych do konataktu (imię, nazwisko, telefon, mail).	Tryb odwołań bezpośrednich	Krytyczny dla sukcesu projektu	REST API

7.2. Kluczowe komponenty architektury rozwiązania



7.3. Przyjęte założenia technologiczne

Lp.	Obszar	Założenie technologiczne
1.	Infrastruktura	wykorzystanie infrastruktury on-premise - ze względu na charakter systemu nie jest możliwe wykorzystanie rozwiązań chmurowych.
2.	Sieć i bezpieczeństwo	zgodność z wytycznymi dotyczącymi systemów do obsługi informacji niejawnych o klauzuli "zastrzeżone" przekazanymi przez ABW w trakcie inspekcji i przeglądów dokumentacji akredytacyjnej - zgodnie z ustawą o ochronie informacji niejawnych. Stosowanie wydzielonych sieci do komunikacji niejawnej. Informacje dotyczące poszczególnych klas zabezpieczeń znajdują się w Kancelarii Tajnej NASK PIB.
3.	Standardy wymiany danych	W obszarze jawnym stosowanie endpointów REST przez HTTP/ HTTPS. Format danych: Json. W obszarze niejawnym protokoły komunikacyjne są dostępne w opisach dokumentacji certyfikacyjnej rozwiazań dostępne w kancelariach tajnych poszczególnych producentów rozwiązań.
4.	Systemy operacyjne serwerowe	W części jawnej zakłada się stosowanie systemów operacyjnych klasy Linux. W części niejawnej specyfikacja stosowanych

Lp.	Obszar	Założenie technologiczne
		rozwiązań jest opisana w dokumentacji akredytacyjnej dostępnej w kancelarii tajnej NASK PIB.
5.	Bazy danych	Zakłada się stosowanie relacyjnych baz danych.
6.	Serwery aplikacji	Zakłada się stosowanie serwerów aplikacyjnych opartych o otwarty kod źródłowy
7.	Portale	Dla e-Usług zakłada się zgodność z WCAG 2.2 poziom (AA). Portal będzie wystawiony w części jawnej systemu.
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~~

Lp.	Rejestr publiczny	Opis	Zakres przetwarzania
1	Wykaz Podmiotów Kluczowych i Podmiotów Ważnych	Wykaz Podmiotów Kluczowych i Podmiotów Ważnych prowadzony w systemie S46 odpowiada za samorejestracje podmiotów kluczowych i ważnych. Umożliwia podmiotom kluczowym i ważnym obsługę cyklu życia wpisu w Wykazie. W szczególności umożliwia: rejestrację, weryfikację statusu wpisu do Wykazu, wskazanie osób właściwych do spraw cyberbezpieczeństwa, czy aktualizację danych dotyczących podmiotu. Ze strony organów właściwych możliwa jest obsługa wniosków o wpis oraz wpisywanie podmiotów kluczowych lub podmiotów ważnych do wykazu z urzędu przez ministra właściwego do spraw informatyzacji i organy właściwe do spraw cyberbezpieczeństwa, czy wykreślenie z Wykazy podmiotów KCS, jak również raportowanie.	Użycie danych

7.5. Bezpieczeństwo

Planowany poziom zapewnienia bezpieczeństwa (w rozumieniu przepisów § 19 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773)) 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

System SKR-Z jest systemem przetwarzającym informacje niejawne i z tego względu podlega odrębnym przepisom dotyczącym akredytacji systemu. Informacje dotyczące zastosowanych mechanizmów bezpieczeństwa są dostępne w dokumentacji akredytacyjnej o klauzuli "zastrzeżone" do wglądu w Kancelarii Tajnej NASK PIB.

~~- dodatkowe zabezpieczenia powyżej wymogów KRI: należy wskazać uzasadnienie~~