# **Szczegółowy opis przedmiotu zamówienia**

# **I. PRZEDMIOT ZAMÓWIENIA**

Przedmiotem zamówienia jest dostawa Oprogramowania wraz z udzieleniem lub zapewnieniem udzielenia licencji, świadczenie Usług Towarzyszących, w tym w szczególności wdrożenie przez Wykonawcę Systemu służącego do weryfikacji, ochrony, monitorowania i alertowania incydentów bezpieczeństwa w zakresie uwierzytelnienia użytkowników, wraz ze wsparciem technicznym i Gwarancją. Wdrożenie obejmować będzie uruchomienie oraz konfigurację zgodnie z wymaganiami Zamawiającego, w zakresie niezbędnym do poprawnego działania Systemu.

1. W ramach przedmiotu zamówienia Wykonawca zobowiązuje się:
   1. dostarczyć Oprogramowanie niezbędne do uruchomienia Systemu,
   2. udzielić lub zapewnić udzielenie wszelkich licencji wymaganych do prawidłowego działania Systemu, jako całości jak i poszczególnych jego elementów dla **90 tysięcy użytkowników** w rozproszonej strukturze. Licencjobiorcą jest Zamawiający, a podmiotami uprawnionymi do korzystania z Systemu są Jednostki.
   3. dostarczyć fizyczne klucze bezpieczeństwa wymagane do prawidłowego działania Systemu, jako całości jak i poszczególnych jego elementów dla **10 tysięcy użytkowników**,
   4. świadczyć Usługi Towarzyszące, w języku polskim, w łącznej maksymalnej ilości 5000 godzin do wykorzystania w całym okresie obowiązywania Umowy ramowej, w tym: Usługi Instalacyjno -Wdrożeniowe w łącznej maksymalnej ilości 2000 godzin, opisane w pkt V.A) OPZ i Usługi Wsparcia Eksperckiego Wykonawcy w łącznej maksymalnej ilości 3000 godzin opisane w pkt V.B) OPZ.
   5. wykonać Dokumentację i przenieść na Jednostkę autorskie prawa majątkowe do Dokumentacji,
   6. zapewnić wsparcie techniczne dla dostarczonego Oprogramowania na okres 36 miesięcy od podpisania odpowiedniego Protokołu odbioru,
   7. udzielić Gwarancji na dostarczone Oprogramowanie, System, a także na nośniki danych i fizyczne klucze bezpieczeństwa na okres 36 miesięcy od podpisania odpowiedniego Protokołu odbioru, oraz świadczyć w tym okresie usługi gwarancyjne w zakresie wdrożonego Systemu.

Zamawiający przewiduje możliwość wdrożenia Systemu w różnych lokalizacjach, konfiguracjach i różnym czasie dostawy w trakcie obowiązywania Umowy ramowej, zgodnie ze złożonymi przez Jednostki Wnioskami o zamówienie.

# **II. WYMAGANIA OGÓLNE**

1. Oferowany System ma stanowić jednolite i kompleksowe rozwiązanie i składać się musi co najmniej z:
   1. **Modułu ochrony tożsamości** zapewniającego funkcjonalność weryfikacji, ochrony, monitorowania i alertowania incydentów bezpieczeństwa w zakresie centralnego procesu uwierzytelnienia użytkowników na bazie polityk bezpieczeństwa i dostępu;
   2. **Modułu fizycznych kluczy bezpieczeństwa** zapewniającego dodatkowy komponent procesu uwierzytelnienia.
2. Moduł ochrony tożsamości musi stanowić jednolite środowisko programowe i pochodzić od jednego Producenta.
3. Moduł fizycznych kluczy bezpieczeństwa musi bezpośrednio integrować się z Modułem ochrony tożsamości i musi pochodzić od tego samego Producenta co Moduł ochrony tożsamości.
4. Wszystkie Moduły Systemu muszą mieć możliwość pracy w środowisku Jednostek bez konieczności stosowania zewnętrznych usług, w szczególności bez wykorzystania publicznej chmury obliczeniowej.
5. System musi mieć możliwość pracy w środowisku bez dostępu do sieci Internet. Nie jest dopuszczalne stosowanie rozwiązań chmurowych, hybrydowych i kolokowanych poza infrastrukturą Jednostek.
6. System musi być skalowalny i elastyczny w kontekście potencjalnej rozbudowy tj. objęcia ochroną kolejnych użytkowników.
7. Każdy Moduł musi posiadać tylko jedną konsolę zarządzającą.
8. Oferowane rozwiązanie nie może być zabronione do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization).
9. Oferowane rozwiązanie nie może być czasowo wstrzymane do stosowania przez administrację któregokolwiek z państw członkowskich NATO (North Atlantic Treaty Organization).
10. Wszystkie elementy Systemu muszą być dostarczone w najnowszej i aktualnej wersji (tzn. najnowszej i aktualnej udostępnionej przez Producenta oferowanego rozwiązania w tym zakresie) na dzień wdrożenia Systemu.
11. Żaden z elementów oferowanego Systemu na dzień składania ofert nie może być przeznaczony przez Producenta do wycofania z produkcji lub sprzedaży.
12. Czynności związane z wdrożeniem i konfiguracją Systemu w infrastrukturze Jednostki muszą być przeprowadzone przez personel Wykonawcy w obecności personelu Jednostki .

# **III. WYMAGANIA W ZAKRESIE MODUŁU OCHRONY TOŻSAMOŚCI**

1. **Wymagania dotyczące oferowanego rozwiązania**
2. Moduł ochrony tożsamości musi zapewniać pracę w trybie wysokiej dostępności (HA w trybie active active), zapewniać nadmiarowość elementów wykonawczych i dostępność.
3. Moduł ochrony tożsamości musi zapewniać ciągłość przetwarzania żądań uwierzytelniania i egzekwowania polityk w przypadku niedostępności konsoli administracyjnej.
4. Moduł ochrony tożsamości w przypadku Awarii, niedostępności wszystkich elementów wykonawczych, musi zapewniać automatyczne obejście skonfigurowanych polityk bezpieczeństwa tożsamości.
5. Moduł ochrony tożsamości musi zapewnić bezpieczną komunikację pomiędzy konsolą administracyjną, a elementami wykonawczymi.
6. Moduł ochrony tożsamości musi zapewniać holistyczną platformę uwierzytelniania, która monitoruje dostęp użytkownika we wszystkich systemach i środowiskach bez instalacji agentów na tych systemach, proxy i lokalnych konfiguracji.
7. Moduł ochrony tożsamości musi zapewniać konsolę dostępną z poziomu przeglądarki internetowej dla administratora w celu konfiguracji i zarządzania.
8. Moduł ochrony tożsamości musi zapewniać aktualizowane rozwiązania z jednej konsoli administracyjnej niezależnie od liczby skonfigurowanych elementów modułu.
9. Moduł ochrony tożsamości nie może wprowadzać istotnych opóźnień czasowych realizacji procesu uwierzytelniania.
10. Moduł ochrony tożsamości nie może mieć dostępu do żadnego hasła podczas analizy ruchu uwierzytelniającego.
11. Moduł ochrony tożsamości musi wspierać powiadamianie na pulpicie w systemach Windows i Mac w przypadku wykorzystania tożsamości użytkownika. Powiadomienie powinno być uruchamiane z sieci wewnętrznej i nie opierać się na dostępie do Internetu.
12. Moduł ochrony tożsamości musi wspierać obsługę spersonalizowanych powiadomień z informacją o kontekście przychodzącego żądania uwierzytelnienia.
13. Moduł ochrony tożsamości musi zapewnić reguły lub polityki zarządzania żądaniami uwierzytelnienia użytkowników w oparciu o zdefiniowane parametry, takie jak protokół, użytkownik, grupa, urządzenie, zasób, poziom wskaźnika ryzyka itp.
14. Moduł ochrony tożsamości musi zapewnić reguły lub polityki zarządzania żądaniami uwierzytelnienia kont usługowych w oparciu o zdefiniowane parametry, takie jak protokół, konto usługowe, zasób, poziom wskaźnika ryzyka itp.
15. Moduł ochrony tożsamości w kontekście użytkowników musi zapewniać możliwość wdrożenia przynajmniej dla rozwiązań Active Directory (Kerberos, NTLM, LDAP, LDAPs), RADIUS, ADFS.
16. Moduł ochrony tożsamości w kontekście kont usługowych musi zapewniać możliwość wdrożenia przynajmniej dla rozwiązań Active Directory (Kerberos, NTLM, LDAP, LDAPs).
17. Moduł ochrony tożsamości musi umożliwiać przeglądanie, alertowanie, analizę i egzekwowanie polityk bezpieczeństwa dotyczących zdarzeń związanych z uwierzytelnieniem pochodzących z wielu repozytoriów tożsamości, w tym dla Active Directory, RADIUS, ADFS.
18. Moduł ochrony tożsamości musi umożliwiać blokowanie zdarzeń związanych z uwierzytelnianiem z wielu repozytoriów tożsamości, w tym dla AD, Azure AD, ADFS, RADIUS.
19. Moduł ochrony tożsamości musi umożliwiać tworzenie polityki prekonfigurowanej bezpośrednio z zarejestrowanych elementów żądań uwierzytelnienia z logów.
20. Moduł ochrony tożsamości musi umożliwiać konfigurację czasu, w którym dana polityka będzie egzekwowana.
21. Moduł ochrony tożsamości musi umożliwiać blokowanie dostępu dla grupy urządzeń niezależnie od podawanych poświadczeń.
22. Moduł ochrony tożsamości musi umożliwiać zastosowanie czasowego wykluczenia z polityk wskazanego użytkownika w przypadku niedostępności urządzenia uwierzytelniającego np. zagubienia klucza uwierzytelniającego.
23. Moduł tożsamości musi zawierać zintegrowany element umożliwiający uruchomienie procesu dodatkowego uwierzytelnienia w postaci aplikacji instalowanej na urządzeniach mobilnych (Android v12, iOS v15 i nowszych), stacjach roboczych (Windows 11 ,MacOS v12 i nowszych) oraz Linux (przynajmniej Ubuntu 20 i nowszy).
24. **Wymagania widoczności procesu uwierzytelniania i administrowania**
25. Moduł ochrony tożsamości musi umożliwiać identyfikację i prezentację zapytań uwierzytelnienia dla określonego użytkownika.
26. Moduł ochrony tożsamości musi umożliwiać identyfikację i prezentację zapytań uwierzytelnienia do wskazanego zasobu dla określonego użytkownika.
27. Moduł ochrony tożsamości musi umożliwiać identyfikację i prezentację wszystkich użytkowników uwierzytelniających się do określonego zasobu.
28. Moduł ochrony tożsamości musi umożliwiać logowanie zdarzeń związanych z obsługą rozwiązania (wprowadzanie zmian w konfiguracji i politykach, logowanie działań administratorów). Moduł musi umożliwiać pobranie logów w formacie CSV.
29. Moduł ochrony tożsamości musi umożliwiać wykrywanie i monitorowanie zmian w zakresie kont uprzywilejowanych użytkowników.
30. Moduł ochrony tożsamości musi umożliwiać wykrywanie i alertowanie procesów uwierzytelnienia w kontekście wykorzystania starszych systemów operacyjnych (przynajmniej Windows 7, Windows 8).
31. Moduł ochrony tożsamości musi umożliwiać wykrywanie i śledzenie zmian w zakresie kont tzw. Shadow admins.
32. Moduł ochrony tożsamości musi umożliwiać automatyczne wykrywanie i monitorowanie zdarzeń związanych z interaktywnym logowaniem dokonywanym przez konta usługowe.
33. Moduł ochrony tożsamości musi umożliwiać identyfikację urządzeń, które są dostępne przy użyciu kont usługowych.
34. **Analiza wskaźników ryzyka i ochrona przed atakami**
35. Moduł ochrony tożsamości musi umożliwiać aktywne analizowanie aktywności użytkownika, np.: na podstawie wykorzystania urządzenia dostępowego, żądania dostępu do wielu zasobów w krótkim czasie, aby skutecznie wykrywać anomalie i zagrożenia oparte na kradzieży tożsamości.
36. Moduł ochrony tożsamości musi umożliwiać automatyczną identyfikację i aktualizację wskaźników ryzyka dla określonego użytkownika na podstawie analizy zachowania i przyznanych uprawnień.
37. Moduł ochrony tożsamości musi umożliwiać automatyczną identyfikację i aktualizację wskaźników ryzyka dla określonego urządzenia wykorzystywanego w procesie uwierzytelnienia.
38. Moduł ochrony tożsamości musi umożliwiać alertowanie i blokowanie uwierzytelniania wykorzystując dynamiczne polityki oparte na ryzyku.
39. Moduł ochrony tożsamości musi umożliwiać wykrywanie ataków typu lateral movement na podstawie ciągłego monitorowania zapytań uwierzytelnienia i analizy aktywności użytkowników/urządzeń.
40. Moduł ochrony tożsamości musi umożliwiać skonfigurowanie automatycznego egzekwowania rygorystycznych polityk dostępu dla użytkowników/urządzeń, którzy na podstawie analizy zachowań zostali sklasyfikowani jako źródło atak typu lateral movement.
41. Moduł ochrony tożsamości musi umożliwiać wykrywanie i alertowanie wielokrotnych prób nieudanego uwierzytelnienia.
42. Moduł ochrony tożsamości musi umożliwiać identyfikację ataków bazujących na wzorcach zachowań takich jak: bruteforce, credential scanning, lateral movement.
43. Moduł ochrony tożsamości musi umożliwiać blokowanie dostępu pomiędzy urządzeniami w przypadku wykrycia incydentu naruszającego próg bezpieczeństwa.
44. Moduł ochrony tożsamości musi umożliwiać generowanie raportu, który zestawia najważniejsze informacje na temat zagrożeń wykrytych w zadanym okresie czasu.
45. Moduł ochrony tożsamości musi oferować narzędzie dla administratora do badania podejrzanej aktywności użytkownika lub urządzenia w sieci. Proponowane rozwiązanie powinno również zapewniać szczegółową oś czasu i graficzną reprezentację działań uwierzytelniających użytkownika lub urządzenia w ciągu ostatniego tygodnia.
46. **Wymagane integracje**
47. Moduł ochrony tożsamości musi umożliwiać integracje z systemami klasy SIEM, co najmniej z Systemem SPLUNK, w celu udostępnienia informacji związanych z logami zdarzeń uwierzytelniania w formacie CEF.
48. Moduł ochrony tożsamości musi posiadać API do interakcji z systemem, takie jak uzyskiwanie informacji, konfigurowanie, wprowadzanie informacji o wskaźnikach ryzyka itp.
49. Moduł ochrony tożsamości musi posiadać API umożlwiające zarządzanie politykami bezpieczeństwa.
50. Moduł ochrony tożsamości musi posiadać API umożliwiające zarządzanie procesem rejestrowania tokenów weryfikacyjnych.
51. **Uwierzytelnianie dwuskładnikowe**
52. Moduł ochrony tożsamości musi umożliwiać wykorzystanie dwóch lub więcej narzędzi autoryzacyjnych, zależnie od ustawień.
53. Moduł ochrony tożsamości musi umożliwiać egzekwowanie uwierzytelnienia dwuskładnikowego dla zdalnych połączeń administracyjnych, co najmniej dla Remote PowerShell, PsExe, Remote Computer Management, Remote Registry, DSC (Desired State Configuration), DCOM (Distributed Component Object Model), WSMAN (Web Services-Management) itp.
54. Moduł ochrony tożsamości musi umożliwiać egzekwowanie uwierzytelnienia dwuskładnikowego na stacji roboczej w przypadku uruchamiania aplikacji na prawach administratora, np. administratora domeny Active Directory.
55. Moduł ochrony tożsamości musi umożliwiać uwierzytelnienie dwuskładnikowe w usłudze katalogowej Active Directory wersji dla systemów Windows Server 2012 i nowszych oraz minimalny poziom funkcjonalny lasu I domeny 2012 i nowszych.
56. Moduł ochrony tożsamości musi umożliwiać uwierzytelnienie dwuskładnikowe dla dostępu do wskazanego zasobu sieciowego udostępnionego z wykorzystaniem protokołu Common Internet File System (CIFS) bez instalacji agenta na serwerze.
57. Moduł ochrony tożsamości musi umożliwiać uwierzytelnienie dwuskładnikowe dla protokołu Remote Desktop Protocol (RDP) bez instalacji agenta na serwerze.
58. Moduł ochrony tożsamości musi umożliwiać uwierzytelnienie dwuskładnikowe dla dostępu zdalnego z wykorzystaniem PowerShell do systemu Windows Server 2012 lub nowszym bez instalacji agenta na serwerze.
59. Moduł ochrony tożsamości musi umożliwiać uwierzytelnienie dwuskładnikowe do baz danych (minimum MS SQL) bez instalacji agenta na serwerze bazy danych.
60. Moduł ochrony tożsamości musi umożliwiać uwierzytelnienie dwuskładnikowe dla dostępu do konsoli centralnej narzędzia do wirtualizacji (tzw. hypervisor jak np.: VMware vCenter, Microsoft Hyper-V) bez konieczności instalacji agenta na serwerach konsoli wirtualizującej.
61. Moduł ochrony tożsamości musi umożliwiać uwierzytelnienie dwuskładnikowe do stacji roboczych Virtual Desktop Infrastructure (VDI) przynajmniej dla Vmware Horizon i Citrix Virtual Dektops.
62. Moduł ochrony tożsamości musi umożliwiać uwierzytelnianie dwuskładnikowe dla połączeń SSH do systemów Linux bez instalacji agenta na tych serwerach.
63. Moduł ochrony tożsamości musi umożliwiać uwierzytelnianie dwuskładnikowe dla rozwiązań do zarządzania uprzywilejowanym dostępem (np. CyberArk, BeyondTrust, Thycotic)
64. Moduł ochrony tożsamości musi umożliwiać uwierzytelnianie dwuskładnikowe dla dostawców VPN, przynajmniej dla rozwiązań Palo Alto Networks i CISCO.
65. Moduł ochrony tożsamości musi umożliwiać uwierzytelnianie dwuskładnikowe dla dostępu do urządzeń sieciowych (routery, switche, zapory sieciowe) wykorzystujące co najmniej protokół RADIUS.
66. Moduł ochrony tożsamości musi umożliwiać uwierzytelnianie dwuskładnikowe dla dostępu do poczty email usługi Exchange i O365.
67. Moduł ochrony tożsamości musi umożliwiać uwierzytelnianie dwuskładnikowe dla dostępu do usługi Outlook Web Access (OWA).
68. Moduł ochrony tożsamości musi umożliwiać uwierzytelnianie dwuskładnikowe dla logowania do stacji roboczej systemu Windows 10 i nowszych, przynajmniej dla FIDO2, oraz OneTimePassword (OTP) w przypadku braku połączenia z Internetem.
69. Moduł ochrony tożsamości musi umożliwiać uwierzytelnianie dwuskładnikowe logowania do stacji roboczej Windows 10 i nowszych z dostępem do Internetu i sieci lokalnej przynajmniej dla FIDO2 i OneTimePassword (OTP).

# **IV. WYMAGANIA MODUŁU FIZYCZNYCH KLUCZY BEZPIECZEŃSTWA**

1. **Wymagania dotyczące oferowanego rozwiązania**
2. Moduł fizycznych kluczy bezpieczeństwa musi wspierać politykę *zero-trust* w środowisku *lokalnym* (on-premises z ograniczonym dostępem do Internetu). Integracja powinna wspierać uwierzytelnianie drugiego czynnika za pomocą certyfikowanych tokenów FIDO2.
3. Moduł fizycznych kluczy bezpieczeństwa musi zapewnić mechanizm dodawania użytkowników i zarządzania ich tokenami weryfikacyjnymi poprzez:
   1. Dostarczenie spersonalizowanej wiadomości e-mail z instrukcjami dla użytkowników w celu samodzielnego dodania tokena weryfikującego,
   2. Zezwolenie lub zablokowanie dostępu użytkownikom, którzy nie ukończyli procesu rejestracji tokena,
   3. Wyświetlanie informacji o użytkownikach dodanych, oczekujących na dodanie i wykluczonych.
4. Moduł fizycznych kluczy bezpieczeństwa musi integrować się bezpośrednio z Modułem ochrony tożsamości w celu użycia fizycznych urządzeń (fizyczne klucze bezpieczeństwa) opisanych w punkcie IX OPZ jako dodatkowego składnika weryfikacji w procesie uwierzytelnienia.

# **V. USŁUGI TOWARZYSZĄCE**

**A) Usługi Instalacyjno-Wdrożeniowe**

1. Usługi Instalacyjno-Wdrożeniowe obejmują:
   1. Instalację i konfigurację dostarczonego Oprogramowania przez Wykonawcę,
   2. Wykonanie Dokumentacji Projektowej, Dokumentacji Powykonawczej i Dokumentacji Testów Akceptacyjnych,
   3. Instalację Oprogramowania w środowisku Jednostki,
   4. Skonfigurowanie Systemu zgodnie z Dokumentacją Projektową, uzgodnioną na etapie Umowy wykonawczej,
   5. Wykonania testów akceptacyjnych wykazujących poprawność wdrożenia Systemu zgodnie z Dokumentacją Projektową, uzgodnioną na etapie Umowy wykonawczej,
   6. przygotowanie procedur obsługi dot. eksploatacji, awarii, wykonania kopii zapasowych oraz ich odtworzenia, administrowania Systemem.
   7. zapewnieniu możliwości udziału osób wskazanych przez Jednostkę przy przeprowadzanym przez inżyniera/inżynierów wdrożeniu Systemu po stronie Wykonawcy.
2. Ilości godzin Usług Instalacyjno-Wdrożeniowych będą każdorazowo rozliczane z łącznej puli godzin przeznaczonej na świadczenie Usług Towarzyszących, na podstawie ilości godzin wskazanych przez Jednostkę we Wniosku o zamówienie.
3. Maksymalna ilość godzin Usług Instalacyjno-Wdrożeniowych wynosi 2000 godzin zegarowych.
4. Usługi Instalacyjno-Wdrożeniowe będą realizowane na podstawie zatwierdzonego przez Jednostkę harmonogramu wdrożenia na zasadach określonych w Umowie ramowej.
5. Termin wykonania Usług Instalacyjno-Wdrożeniowych będzie precyzowany przez Jednostkę we Wniosku o zamówienie.
6. Na wniosek Wykonawcy Jednostka może wyrazić zgodę w formie elektronicznej (e-mail) lub dokumentowej na wykonanie prac instalacyjno-wdrożeniowych zdalnie w całości lub części, pod warunkiem przestrzegania przez Wykonawcę zasad bezpieczeństwa określonych przez Wykonawcę. Jednostka ma prawo odmowy udostępnienia zdalnego dostępu w dowolnym momencie bez podawania przyczyny.
7. Wykonawcy nie przysługuje dodatkowe wynagrodzenie ani zwrot poniesionych jakichkolwiek kosztów z tytułu realizacji prac w siedzibie Jednostki/Jednostek, w których odbywa się wdrożenie.
8. Jednostka dostarczy uzgodnione z Wykonawcą zasoby informatyczne potrzebne do instalacji i wdrożenia elementów rozwiązania.
9. Wykonawca przeprowadzi, na etapie wdrożenia Systemu, Warsztaty Wdrożeniowe w języku polskim dla maks. 25 uczestników w zakresie obsługi i administracji wdrażanego Systemu w wymiarze minimum 16 godzin zegarowych.
10. Warsztaty Wdrożeniowe stanowią element Usług Instalacyjno – Wdrożeniowych i polegać będą w szczególności na:
    * 1. przeprowadzeniu warsztatów w formie online,
      2. udzielaniu odpowiedzi na pytania w zakresie zagadnień związanych z czynnościami administracyjnymi, funkcjonowaniem wdrożonego rozwiązania w środowisku produkcyjnym,
      3. zapewnieniu transferu wiedzy obejmującego swoim zakresem wiedzę dot. dostarczanego Systemu i przygotowanie uczestników w zakresie administrowania, utrzymania i rozwiązywania problemów dot. Systemu.
11. Wykonawca zapewni możliwość konsultowania z trenerami tematów omawianych podczas Warsztatów Wdrożeniowych oraz opieki merytorycznej nad uczestnikami Warsztatów Wdrożeniowych w okresie 5 dni roboczych po ich zakończeniu za pomocą poczty elektronicznej (udzielanie odpowiedzi drogą elektroniczną na pytania lub wątpliwości powstałe podczas Warsztatów).
12. Wszystkie koszty z wiązane z organizacją, przeprowadzeniem, zapewnieniem materiałów szkoleniowych itp. pokrywa Wykonawca.
13. Potwierdzeniem prawidłowej realizacji wdrożenia, uruchomienia i skonfigurowania Systemu będzie podpisany bez zastrzeżeń Protokół Odbioru Wdrożenia Systemu, zawierający w szczególności:
    1. odbiór Systemu wraz z Modułami i komponentami, na podstawie Dokumentacji Projektowej i przeprowadzonych Testów Akceptacyjnych,
    2. odbiór Dokumentacji Powykonawczej,
    3. odbiór realizacji Warsztatów Wdrożeniowych.

**B) Usługi Wsparcia Eksperckiego** **Wykonawcy**

1. Usługi Wsparcia Eksperckiego Wykonawcy będą obejmowały:
   1. bieżące utrzymanie, zarządzanie i administrowanie oferowanym przez Wykonawcę Systemem,
   2. przeprowadzenie konsultacji, instruktażu, rozwiązywanie bieżących problemów związanych z obsługą, w tym instalacją, konfiguracją, optymalizacją, utrzymaniem i administracją Systemu, z wyłączeniem Awarii usuwanych w ramach Gwarancji oraz z wyłączeniem czynności wykonywanych w ramach Wsparcia Technicznego,
2. Rodzaj Usług Wsparcia Eksperckiego Wykonawcy będzie precyzowany na etapie zlecenia z zastrzeżeniem pkt 1 powyżej.
3. Ilości godzin Usług Wsparcia Eksperckiego Wykonawcy będą każdorazowo rozliczane z łącznej puli godzin przeznaczonej na świadczenie Usług towarzyszących na podstawie ilości godzin wskazanych przez Zamawiającego we Wniosku o zamówienie.
4. Maksymalna ilość godzin wsparcia eksperckiego wynosi 3000 godzin zegarowych.
5. Usługi Wsparcia Eksperckiego Wykonawcy będą realizowane na podstawie zatwierdzonego przez Zamawiającego harmonogramu realizacji Usług Wsparcia Eksperckiego Wykonawcy, na zasadach określonych w Umowie ramowej.
6. Maksymalny termin wykonania Usług Wsparcia Eksperckiego Wykonawcy będzie precyzowany przez Jednostkę we Wniosku o zamówienie.
7. Potwierdzeniem prawidłowej realizacji Usług Wsparcia Eksperckiego Wykonawcy, będzie podpisany bez zastrzeżeń Protokół Odbioru Usług.

# **VI. Wymagania w zakresie Gwarancji i wsparcia technicznego**

**A) GWARANCJA**

1. W ramach udzielonej Gwarancji Wykonawca udostępni oprogramowanie umożliwiające zdalne zgłaszanie i monitorowanie statusu Zgłoszenia Serwisowego Awarii, oprogramowanie to musi zapewnić Jednostce brak ograniczeń, co do liczby dokonywanych Zgłoszeń Serwisowych w zakresie Awarii.
2. Wszelkie prace wykonywane przez Wykonawcę w Systemie nie mogą skutkować utratą praw gwarancyjnych do Systemu.
3. W ramach udzielonej gwarancji Wykonawca będzie rozwiązywał zgłaszane problemy związane z działaniem i obsługą Systemu, to jest realizował Zgłoszenia Serwisowe Awarii w następujący sposób:
   1. **Awaria Krytyczna**, wada skutkująca nieprawidłowym działaniem dowolnego elementu rozwiązania powodująca albo całkowity brak możliwości korzystania albo takie ograniczenie możliwości korzystania, że rozwiązanie przestaje spełniać swoje podstawowe funkcje. Czas odnalezienia obejścia lub Naprawy do 12 godzin od chwili Zgłoszenia Serwisowego przez Jednostkę;
   2. **Awaria Niekrytyczna** wada skutkująca nieprawidłowym działaniem dowolnego elementu rozwiązania powodująca ograniczenie korzystania z rozwiązania, nie powodując skutków opisanych dla Awarii Krytycznej. Czas odnalezienia obejścia lub Naprawy do 72 godzin od chwili Zgłoszenia Serwisowego przez Jednostkę.
4. Wszelkie Awarie będą zgłaszane przez Jednostkę za pomocą udostępnionego przez Wykonawcę oprogramowania o którym mowa w punkcie 1 powyżej.
5. W przypadku potrzeby konsultacji z działem wsparcia technicznego Producenta lub wydania poprawki przez Producenta, na wniosek Wykonawcy złożony w formie elektronicznej, Jednostka zawiesi czas usunięcia Awarii do czasu udostępnienia poprawki lecz nie dłużej niż 90 dni.

**B) WSPARCIE TECHNICZNE**

1. Wsparcie techniczne musi obejmować co najmniej:
2. aktualizację i konfigurację Oprogramowania przez Wykonawcę,
3. instalację poprawek, usprawnień i nowych wersji Oprogramowania, udostępnianych przez Producenta, na wezwanie i w terminie uzgodnionym z Jednostką.
4. W ramach udzielonej gwarancji Jednostce przysługuje prawo do samodzielnej instalacji i używania wszystkich poprawek, usprawnień i nowych wersji Systemu udostępnianych przez jego Producenta bez ponoszenia dodatkowych kosztów finansowych. Powyższe nie może skutkować utratą uprawnień gwarancyjnych przysługujących Jednostkom.

# **VII. Wymagania w zakresie Dokumentacji Projektowej**

Wykonawca w uzgodnieniu z Jednostką (Zespołem Odbiorowym) opracuje i dostarczy następującą Dokumentację Projektową:

1. Projekt Wdrożenia Systemu, który musi zawierać, w szczególności: opis funkcjonalny, wykaz wymaganych elementów Systemu, sposób ich wdrożenia i konfiguracji, wykaz licencji niezbędnych dla działania Systemu jako całości, szczegółowy opis architektury proponowanego rozwiązania wraz z opisem integracji z infrastrukturą techniczną Jednostki, harmonogram wdrożenia,
2. Dokumentację Testów Akceptacyjnych wdrożenia Systemu, która musi dokumentować działania, jakie należy wykonać, aby uzyskać potwierdzenie, że wdrożony System jest zgodny z opisem przedmiotu zamówienia. Testy Akceptacyjne mają być realizowane w środowisku produkcyjnym, zgodnie ze scenariuszami testowymi opracowanymi przez Wykonawcę i zaakceptowanymi przez Jednostkę (Zespół Odbiorowy) na etapie odbioru Dokumentacji Projektowej.

Dokumentacja musi być dostarczona w wersji elektronicznej i napisana w języku polskim.

Procedury i instrukcje Producenta mogą być dostarczone w języku angielskim lub polskim.

Potwierdzeniem prawidłowej realizacji Dokumentacji Projektowej, będzie podpisany bez zastrzeżeń Protokół Odbioru Projektu zawierający w szczególności: odbiór Projektu Wdrożenia Systemu i Dokumentacji Testów Akceptacyjnych.

## **VIII. Wymagania w zakresie Dokumentacji Powykonawczej**

Dokumentacja Powykonawcza ma zawierać, w szczególności:

* + - 1. Szczegółową konfiguracją oraz opis infrastruktury technicznej wdrażanego Systemu,
      2. Opis struktury i konfiguracji Systemu,~~,~~
      3. Zalecenia i procedury eksploatacyjne oraz zalecenia w zakresie konserwacji Systemu~~,~~
      4. Wykonawca opracuje i dostarczy Dokumentację Powykonawczą, która musi być jednym spójnym dokumentem, bez względu na jej objętość i musi zawierać procedury administracyjne i operacyjne oraz inne informacje, istotne w eksploatacji rozwiązania, w szczególności:

1. procedury i instrukcje dotyczące instalacji, konfiguracji i aktualizacji,
2. procedury dotyczące wykonywania i przechowywania kopii bezpieczeństwa,
3. instrukcje dla użytkowników i administratorów,
4. inne niezbędne dokumenty, jakie powstaną w trakcie realizacji wdrożenia, uzgodnione z Jednostką (Zespołem Odbiorowym).
   * + 1. Dokumentacja Powykonawcza musi być dostarczona w wersji elektronicznej i napisana w języku polskim. Procedury i instrukcje Producenta mogą być dostarczone w języku angielskim lub polskim.
       2. Potwierdzeniem prawidłowej realizacji Dokumentacji Powykonawczej, będzie podpisany bez zastrzeżeń Protokół Odbioru Wdrożenia Systemu.

## **IX Wymagania dla fizycznych kluczy bezpieczeństwa**

1. Urządzenie musi być rozwiązaniem sprzętowym skutecznie chroniącym m.in. przed phishingiem.
2. Urządzenie musi posiadać wsparcie dla platform: Microsoft Windows, Mac OS, Linux.
3. Urządzenie musi być kompatybilne z przeglądarkami: Chrome, Edge, Opera, Safari, Firefox.
4. Urządzenie musi posiadać możliwość potwierdzenia logowania tj. - obowiązkowa interakcja użytkownika z urządzeniem podczas weryfikacji procesu logowania.
5. Urządzenie musi posiadać wsparcie dla PKCS#11.
6. Urządzenie musi obsługiwać algorytmy kryptograficzne: RSA 2048, RSA 4096 (PGP), ECC p256, ECC p384.
7. Urządzenie musi być odporne na fizyczne uszkodzenie takie jak np. zgniecenie.
8. Urządzenie musi posiadać klasę szczelności IP68.
9. Urządzenie do działania nie może wymagać baterii.
10. Urządzenie do działania nie może wymagać połączenia internetowego.
11. Urządzenie nie może być rozwiązaniem typu pendrive, czyli posiadać miejsce do przechowywania danych: pliki, katalogi.
12. Urządzenie nie może wykorzystywać standardu Bluetooth.
13. Urządzenie musi być tak fizycznie skonstruowane, by uniemożliwić jego rozłożenie na części i ponowne złożenie.
14. Urządzenie musi posiadać certyfikację U2F i FIDO2 do dwustopniowego uwierzytelniania.
15. Urządzenie musi być tak zabezpieczone przez producenta, że nie ma możliwości wykonania jego kopii na inny klucz czy też dokonania manipulacji w obrębie jego oprogramowania.
16. Oprogramowanie do zarządzania urządzeniem musi być udostępnione do pobrania ze strony producenta.
17. Urządzenie musi posiadać oprócz U2F i FIDO2 również inne możliwości logowania czy obsługi szyfrowania, jak: smart card, Open PGP, OTP, kody zdarzeniowe i czasowe TOTP/HOTP, statyczne hasło oraz Challenge-Response.
18. Urządzenie musi posiadać możliwość zaprogramowania dwóch dodatkowych portów o dodatkowe funkcje:
    1. OTP (przechowywanie kodów na kluczu sprzętowym do odczytu za pomocą aplikacji producenta)
    2. kody zdarzeniowe i czasowe TOTP/HOTP (przechowywanie kodów na kluczu sprzętowym do odczytu za pomocą aplikacji producenta)
    3. statyczne hasło
    4. Challenge-Response
19. Oprogramowania/biblioteki/API na stronie Producenta muszą być dostępne na zasadzie open source, w celu integracji z niestandardowymi aplikacjami.
20. Moduł fizycznych kluczy bezpieczeństwa musi integrować się bezpośrednio z Modułem ochrony tożsamości w celu użycia opisanych kluczy jako dodatkowego składnika weryfikacji w procesie uwierzytelnienia.