Zapytanie ofertowe
dotyczące zakupu subskrypcji oprogramowania do uwierzytelniania dwuskładnikowego w systemie pocztowym wraz ze wsparciem technicznym

Zamawiający:
Ministerstwo Rozwoju i Technologii
Pl. Trzech Krzyży 3/5
00-507 Warszawa

OPIS PRZEDMIOTU ZAMÓWIENIA

I. PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest zakup subskrypcji oprogramowania do uwierzytelnienia dwuskładnikowego w systemie pocztowym na okres 12 miesięcy.

W związku z realizacją przedmiotu Zamówienia Wykonawca dostarczy Zamawiającemu oprogramowanie i usługi zgodnie z poniższym wykazem lub równoważne zgodnie z warunkami określonymi w rozdziale III.

Lp.	Produkt	Liczba produktów
1	Subskrypcja na 1 węzeł Secfence wraz ze wsparciem technicznym producenta na okres 12 miesięcy	1 węzeł
2	Subskrypcja na chronione konta	100 kont
3	Usługi asysty technicznej	40 roboczogodzin

II. TERMIN REALIZACJI ZAMÓWIENIA

Dostawa subskrypcji oprogramowania zostanie zrealizowana w terminie do 10 dni od daty podpisania umowy.

W terminie do 10 dni od dnia zawarcia umowy Wykonawca zapewni dostęp do spersonalizowanej strony pozwalającej upoważnionym ze strony Zamawiającego osobom na:

a) pobieranie aktywowanie bieżącej, pełnej wersji oprogramowania wymienionego w tabeli oprogramowania,

b) pobieranie kluczy aktywacyjnych do oprogramowania,

c) bezpłatne pobieranie poprawek bezpieczeństwa;

d) bezpłatne pobieranie poprawek błędów krytycznych;

e) dostęp do zespołu wsparcia Producenta dedykowanego do rozwiązywania problemów technicznych.

III. MINIMALNE WYMAGANIA SUBSKRYPCJI oprogramowania do uwierzytelniania dwu-składnikowego w systemie pocztowym.

Zamawiający posiada wdrożony system pocztowy Outlook. System pocztowy skonfigurowany jest na licencjach serwerowych w wersji MS Exchange 2019.

Poniżej opisano minimalne wymagania, które muszą spełniać subskrypcje oprogramowania do uwierzytelnienia dwuskładnikowego w systemie pocztowym Zamawiającego.

1. Oprogramowanie musi posiadać mechanizm i możliwość wprowadzenia zabezpieczenia procesu uwierzytelnienia dostępu do Chronionego systemu (dostępnego przez przeglądarkę internetową) poprzez zastosowanie dodatkowego składnika weryfikującego tożsamość użytkownika.

2. Oprogramowanie musi wspierać standard 2FA w postaci haseł jednorazowych generowanych przez aplikacje oraz fizyczne Klucze Zabezpieczające z interfejsami USB oraz wykorzystujące technologię NFC.
3. Zamawiający wymaga udostępnienia wraz subskrypcją oprogramowania 10 szt. kluczy kryptograficznych w standardzie U2F – z obsługą protokołu NFC.
4. Klucze muszą pasować do gniazd USB typu A.
5. Operacja wydania poświadczenia musi następować w wyniku dotknięcia płytki pojemnościowej wbudowanej w klucz kryptograficzny lub poprzez zbliżenie klucza do anteny NFC wbudowane w urządzenia czytniki biometryczne, których obsługa nie wymaga stosowania dodatkowego middleware do działania z oprogramowaniem.
6. Podczas realizacji etapu rejestracji i weryfikacji drugiego składnika oprogramowanie musi komunikować się wyłącznie z infrastrukturą Zamawiającego. W procesie uwierzytelniania niedopuszczalna jest komunikacja poza infrastrukturę Zamawiającego.
7. Oprogramowanie musi pracować w ramach infrastruktury zamawiającego bez konieczności dostępu do usług zlokalizowanych poza infrastrukturą zamawiającego.
8. Niedopuszczalne jest wywoływanie API/SDK w systemach poza infrastrukturą zamawiającego.
9. Oprogramowanie i wszystkie jego komponenty, muszą być aktualnie obecne w linii produktowej producenta i jednocześnie nie mogą znajdować się na liście „end-of-sale”, „end-of-life” oraz „end-of-support” producenta dostarczanej technologii.
10. Oprogramowanie musi zapewniać ochronę (za pomocą 1.2.1, 1.2.2 oraz 1.2.3) dla nieograniczonej ilości Chronionych systemów/serwisów Zamawiającego

Ww. zakres został opisany z wykorzystaniem ilości Tożsamości użytkowników Chronionych systemów.

Oprogramowanie będą podlegać również użytkownicy aplikacji, które nie przechowują tożsamości użytkowników w centralnym repozytorium tożsamości jak np. Active Directory. Zatem oprogramowanie musi być niezależne od centralnego repozytorium tożsamości.

Rodzaj platformy oprogramowania
1. Oprogramowanie musi funkcjonować w formie Wirtualnego appliance pracującego w środowisku wirtualnym Zamawiającego VMWare w wersji 6 i 7 oraz wspierać technologię Vmware HA (High availability) oraz FT(Fault tolerance)
2. Za Wirtualny appliance w pełni musi odpowiadać producent oprogramowania – w tym za poprawki bezpieczeństwa i aktualizacje.
3. Oprogramowanie musi umożliwiać dołożenie drugiego składnika uwierzytelniania do każdej aplikacji WWW Zamawiającego dostępnej przez przeglądarkę internetową po protokole HTTP/HTTPS niezależnie od technologii, w jakiej aplikacja została wykonana.
4. Oprogramowanie musi umożliwiać obsługę wielu standardów drugiego składnika uwierzytelniania. Na moment dostarczenia wymagana jest możliwość użycia co najmniej U2F/FIDO2, haseł jednorazowych generowanych przez aplikacje (np. Google Authenticator, Authy, inna aplikacja generująca kody jednorazowe zgodna z RFC 6238).
5. Obsługa standardu WebAuthn, co za tym idzie możliwość dopuszczenia lokalnych autentykatorów (np. czytniki biometryczne w smartfonach/laptopach) jako drugi składnik uwierzytelniania.
6. Oprogramowanie musi zapewniać możliwość jednoczesnej obsługi różnych typów drugiego składnika uwierzytelniania w ramach chronionej aplikacji.
7. Administrator musi mieć możliwość edycji listy typów drugiego składnika dostępnych dla użytkowników chronionej aplikacji.
8. Oprogramowanie musi udostępniać sposób rejestracji drugiego składnika uwierzytelniania dla dużej grupy użytkowników bez konieczności ręcznego przypisywania drugiego składnika uwierzytelniania do użytkownika przez administratorów - tzw. self-enrollment.
9. Oprogramowanie musi umożliwiać pełną ochronę aplikacji. Pełna ochrona ma polegać na tym, że użytkownik powinien być dopuszczony do panelu logowania lub jakiegokolwiek innego elementu aplikacji dopiero po poprawnym uwierzytelnieniu się drugim składnikiem.W takim modelu działania, system nie może wymagać podania hasła aplikacji przed poprawnym uwierzytelnieniem drugim składnikiem
10. Oprogramowanie musi rozpoznawać akcję wylogowania użytkownika z chronionej aplikacji i co za tym idzie, natychmiast unieważniać sesję na poziomie Oprogramowania.
11. Musi istnieć możliwość ustawienia czasu, na jaki zostaje wydany dostęp do aplikacji objętej pełną ochroną. Po wygaśnięciu tego czasu użytkownik musi zostać ponownie proszony o uwierzytelnienie drugim składnikiem.
12. Oprogramowanie musi mieć możliwość modyfikacji nagłówków HTTP związanych z bezpieczeństwem aplikacji, w szczególności:
    - możliwość nadpisania/modyfikowania Content-Security-Policy bez zmian w chronionej aplikacji ani w serwerach HTTP serwujących chronioną aplikację,

- możliwość dodania/nadpisania nagłówka HSTS bez zmian w chronionej aplikacji ani w serwerach HTTP serwujących chronioną aplikację.

Awaryjny dostęp do chronionych aplikacji:

1. Oprogramowanie musi umożliwiać generowanie jednorazowych kodów dla użytkowników, którzy z losowych powodów nie mogą uwierzytelnić się zarejestrowanym drugim składnikiem.
2. Musi być możliwość konfiguracji długości oraz czasu aktywności kodu jednorazowego dla chronionej aplikacji.
3. Musi być możliwość konfiguracji ilości nieudanych prób, po których kod jednorazowy będzie automatycznie unieważniany.
4. Musi być możliwość definiowania każdorazowo czasu ważności kodu jednorazowego wydawanego użytkownikowi.

Warunkowe zaufanie dla środowiska użytkownika:

1. Oprogramowanie musi umożliwiać włączenie opcji zaufania w przeglądarce na wskazanym urządzeniu. Po zaufaniu przeglądarce użytkownik nie będzie proszony o uwierzytelnienie się drugim składnikiem przez określony czas.
2. Możliwość zaufania w przeglądarce musi być konfigurowalna dla każdej chronionej aplikacji.
3. Czas, na jaki przeglądarka ma zostać oznaczona jako zaufana, musi być konfigurowalny przez administratora oprogramowania.
4. Musi istnieć możliwość definiowania różnego czasu zaufania w przeglądarce dla różnych Chronionych aplikacji.
5. Wsparcie dla dodatkowych protokołów i środowisk.
6. Rozwiązanie musi posiadać wsparcie dla protokołu RADIUS w zakresie uwierzytelniania drugiego składnika, ale w taki sposób, aby oprogramowanie nie przetwarzało hasła wykorzystywanego w pierwszym etapie uwierzytelniania
7. Oprogramowanie musi umożliwiać dodanie drugiego składnika uwierzytelniania w ramach systemu SSO z wykorzystaniem protokołu Kerberos bez ingerencji w kod Chronionych aplikacji, KDC (key distribution center) ani środowisko pracy użytkownika.
8. Oprogramowanie musi umożliwiać przeniesienie wszystkich swoich funkcjonalności z wirtualnego appliance do środowiska kontenerów, w sposób polegający na przekazaniu Zamawiającemu obrazów kontenerów (wraz z opisem architektury), które zostaną zaimportowane do środowiska orkiestrującego kontenerami.
9. Oprogramowanie musi dopuszczać działanie w modelu active/active w co najmniej dwu węzłowym klastrze niezawodnościowym..
10. Dostarczone subskrypcje oprogramowania, oprogramowanie oraz licencje powinny umożliwiać uruchomienie u Zamawiającego minimum 1 węzła oprogramowania. .
11. Oprogramowanie musi umożliwiać pracę pojedynczego węzła przy przepustowości minimum 500Mbps.
12. Oprogramowanie musi umożliwiać ochronę (w zakresie uwierzytelniania) systemów wykorzystujących technologię IPv4.
13. Oprogramowanie musi zapewniać możliwość wysyłania zdarzeń bezpieczeństwa (audyt i zarejestrowane zdarzenia bezpieczeństwa) w postaci logów do zewnętrznych systemów klasy SIEM.
14. Oprogramowanie musi mieć wewnętrzne mechanizmy do monitorowania wydajności i dostępności poszczególnych jego zasobów wraz z możliwością powiadamiania zewnętrznych systemów (typu Nagios) lub administratorów o wystąpieniu problemów.
15. Oprogramowanie musi posiadać moduł logowania zdarzeń.
16. Moduł logowania zdarzeń musi mieć możliwość wysyłania logów do zewnętrznego serwera syslog.
17. Moduł logowania zdarzeń musi logować zdarzenia zachodzące w chronionych aplikacjach, w szczególności:
    a) rejestracja nowego drugiego składnika dla użytkownika,
    b) poprawne zalogowanie za pomocą drugiego składnika,
    c) zalogowanie za pomocą jednorazowego kodu wygenerowanego dla potrzeb awaryjnego dostępu,
    d) nieudane logowanie za pomocą jednorazowego kodu wygenerowanego dla potrzeb awaryjnego dostępu,
    e) dostęp do silnie chronionej części aplikacji.
18. Każdy wpis w dzienniku zdarzeń dotyczący zdarzeń w chronionych aplikacjach musi zawierać co najmniej: nazwę użytkownika i nadzorcy (jeśli dotyczy), czas zdarzenia, adres IP, rodzaj i identyfikator użytego drugiego składnika.
19. Moduł logowania zdarzeń musi logować zdarzenia zachodzące w ramach konfiguracji oprogramowania, w szczególności:
    a) rejestracja nowej aplikacji,

b) dodanie/usunięcie użytkownika panelu administracyjnego,
c) wszystkie zmiany w ramach konfiguracji oprogramowania,
d) logowanie do panelu administracyjnego/API.

Zarządzanie

1. Oprogramowanie musi umożliwiać zarządzanie za pomocą interfejsu graficznego.
2. Panel zarządzania musi mieć możliwość ochrony dostępu administratorów przez wieloskładnikowe uwierzytelnianie, w tym w standardzie FIDO2.
3. Oprogramowanie musi wspierać połączenia bezpiecznym kanałem szyfrowanym z wykorzystaniem SSL/TLS.
4. Musi umożliwiać różnicowanie dostępu dla różnych administratorów.
5. Musi pozwalać na zdefiniowanie min. 10 administratorów, mogących pracować równolegle.
6. Oprogramowanie musi umożliwiać użytkownikom chronionej aplikacji zarządzanie przypisanymi do użytkownika dodatkowymi składnikami uwierzytelniania. Co najmniej: przeglądanie, dodawanie i usuwanie.
7. Interfejs do zarządzania dodatkowymi składnikami uwierzytelniania musi być dostępny dla użytkownika w kontekście interfejsu chronionej aplikacji po zalogowaniu się do niej.
8. Zarządzanie konfiguracją musi być możliwe za pomocą dedykowanego panelu administracyjnego i poprzez API.
9. Panel administracyjny musi umożliwiać granulację uprawnień.
10. Granulacja uprawnień na poziomie panelu administracyjnego powinna umożliwiać dowolne przypisywanie użytkownikowi administracyjnemu ról, co najmniej:
    a) administratora oprogramowania (pełny dostęp),
    b) administratora wybranych aplikacji (zarządzanie konfiguracją wybranych aplikacji i użytkownikami w tych aplikacjach),
    c) wsparcia technicznego dla wybranych aplikacji (zarządzanie użytkownikami w wybranych aplikacjach, np. usuwanie drugiego składnika, generowanie jednorazowych kodów, dostęp do logów niezbędnych do rozwiązywania problemów użytkownika końcowego chronionej aplikacji).
11. Wszystkie akcje dostępne poprzez panel administracyjny muszą być dostępne poprzez API.
12. API musi pozwalać na automatyzację podstawowych zadań administracyjnych (np. wykonywanie kopii zapasowej konfiguracji oprogramowania).

Polityki dostępu dla użytkowników Chronionych aplikacji:

1. Oprogramowanie musi mieć możliwość stosowania różnych polityk dotyczących logowania. Co najmniej:
    a) dobrowolna rejestracja drugiego składnika uwierzytelniania - w takim przypadku użytkownicy powinni być proszeni o rejestrację drugiego składnika, ale dopuszczona jest możliwość logowania bez zarejestrowanego drugiego składnika uwierzytelniania. Użytkownicy, którzy już zarejestrowali drugi składnik uwierzytelniania, nie mogą się zalogować bez dodatkowego uwierzytelnienia,
    b) wymagana rejestracja drugiego składnika uwierzytelniania - w takim przypadku oprogramowanie nie może pozwolić na zalogowanie się użytkownika, który nie zarejestrował drugiego składnika uwierzytelniania,
    c) rejestracja wybiórcza - oprogramowanie wymaga zarejestrowania i używania drugiego składnika uwierzytelniania dla wybranych, nazwanych użytkowników (np. dla użytkowników o podwyższonych uprawnieniach w chronionej aplikacji),
    d) ograniczanie dostępu - oprogramowanie dopuszcza rejestrację drugiego składnika i logowanie do Chronionej aplikacji tylko wybranym, nazwanym użytkownikom.
2. W przypadku punktów c oraz d - użytkownicy podlegający politykom dostępu muszą być dodawani przez API.

Pozostałe wymagania, które musi spełniać zaoferowane oprogramowanie

1. Po stronie użytkownika nie może zachodzić konieczność instalacji dodatkowego oprogramowania (prócz Aplikacji na urządzenia mobilne, które umożliwiają skorzystanie z drugiego składnika uwierzytelniającego) w celu uwierzytelnienia dostępu do Chronionego systemu.
2. Oprogramowanie powinno wspierać aplikacje z wbudowanymi w serwis bazami użytkowników i wykorzystywać wyłącznie tę bazę w procesie pierwszego kroku uwierzytelniania (nazwa użytkownika i hasło). Pierwszy krok uwierzytelniania nie może zakładać uwierzytelnienia w dodatkowej bazie użytkowników ani federację tożsamości użytkowników do zewnętrznych dostawców tożsamości.
3. Możliwość włączenia dodatkowej ochrony wybranych zasobów i akcji (np. odsłonięcie danych wrażliwych jak nr dokumentu tożsamości itp.) w chronionej aplikacji poprzez wymuszenia

dodatkowej i warunkowej autoryzacji za pomocą oprogramowania. Ta dodatkowa i warunkowa autoryzacja ma być przyznana w rezultacie ponownego poświadczenia tożsamości przy próbie wykonania chronionej akcji lub przy dostępie do chronionego zasobu. Po udzieleniu dostępu do chronionego zasobu, autoryzacja ma zostać wycofana, a jej ponowne przyznanie (każdorazowo) ma wymagać ponownego poświadczenia tożsamości za pomocą oprogramowania. Implementacja tej funkcjonalność powinna być realizowana bez ingerencji w kod i konfiguracje Chronionej aplikacji i powinna wspierać co najmniej następujące metody HTTP: GET, POST, PUT, PATCH, DELETE. Dodatkowo powinna być możliwość włączenia ochrony wybranych zasobów lub akcji na zasadzie wprowadzenia dodatkowego nadzorcy czyli do wykonania wybranej akcji ma być dodatkowo wymagane akceptowanie przez drugiego użytkownika (o odpowiednich uprawnieniach).

4. Możliwość dostosowania ekranów związanych z silnym uwierzytelnianiem w zakresie treści i wyglądu, aby móc dopasować ekrany do identyfikacji wizualnej zamawiającego
5. Oprogramowanie musi umożliwiać wdrożenie silnego uwierzytelniania w aplikacjach uwierzytelniających użytkowników w ramach protokołu Kerberos bez ingerencji w kod tych aplikacji.
6. Oprogramowanie musi mieć możliwość łączenia aplikacji w grupy, aby umożliwić przekazanie informacji o silnym uwierzytelnieniu użytkownika w jednej aplikacji pozostałym aplikacjom w grupie.
7. Oprogramowanie musi integrować się z interfejsem chronionej aplikacji zarówno w procesie logowania przy użyciu drugiego składnika uwierzytelniania, jak i przy rejestracji drugiego składnika uwierzytelniania dla nowego użytkownika. Ww. integracja rozumiana jest jako działanie w zakresie tej samej domeny aplikacji i interfejsu chronionej aplikacji. Niedopuszczalne jest przeniesienie użytkownika poza kontekst chronionej aplikacji, do której się loguje (przez kontekst rozumie się ten sam protokół, domenę i port co chronionej aplikacji).
8. Wykonawca po dostarczeniu subskrypcji wesprze Zamawiającego we wdrożeniu i konfiguracji dostarczonej subskrypcji oprogramowania,
9. Wdrożenie oprogramowania nie może wymagać zmian w architekturze technicznej w chronionych aplikacjach.
10. Wdrożenie oprogramowania nie może wymagać integracji z API chronionych aplikacji.
11. Wdrożenie oprogramowania nie może wymagać integracji z usługami dostarczającymi tożsamość.
12. Po wdrożeniu i konfiguracji Wykonawca przeprowadzi instruktaż w zakresie korzystania z oprogramowania, w taki sposób, aby każda z osób uczestniczących w instruktażu posiadała wiedzę i umiejętności potrzebne do prawidłowej obsługi i samodzielnej konfiguracji oprogramowania, z wykorzystaniem jego wszystkich funkcjonalności. Zamawiający będzie wymagał przeprowadzenia takiego instruktażu przez co najmniej jedną osobę, która w okresie dwóch lat przed realizacją instruktażu ukończyła szkolenie oferowane przez producenta oprogramowania, w zakresie objętym instruktażem oraz legitymuje się certyfikatem potwierdzającym ukończenie takiego szkolenia. Równoważnym do powyższego jest wykonanie ww. usługi przez samego producenta oprogramowania, wówczas wszystkie warunki określone w niniejszym punkcie uznaje się za spełnione.
13. Dostarczone oprogramowanie nie może wymagać obsługi standardów SAML/OpenID/OAuth od chronionych aplikacji.
14. Nie dopuszcza się, aby oprogramowanie przechowywało hasła użytkowników do Chronionych aplikacji w jakiejkolwiek formie.

Wymagania w zakresie świadczenia usług wsparcia technicznego

1. subskrypcje oprogramowania muszą zostać dostarczone wraz ze wsparciem technicznym producenta na okres 12 miesięcy.
2. usługi wsparcia producenta muszą obejmować nieograniczony dostęp do wszystkich udostępnionych przez Producenta aktualizacji, poprawek, komunikatów, subskrypcji, baz sygnatur, dokumentacji technicznej, baz wiedzy, instrumentów zgłaszania błędów.
3. Dostęp do uaktualnień sygnatur/reguł i poprawek i aktualizacji licencji/oprogramowania będzie realizowany poprzez udostępnione konto, umożliwiające samodzielne pobieranie uaktualnień sygnatur/reguł oraz poprawek i aktualizacji oprogramowania w ramach posiadanej licencji oraz umożliwiające zakładanie zgłoszeń serwisowych w trybie 24/7/365.
4. konsultacje dot. utrzymania, eksploatowania oraz analizy zdarzeń bezpieczeństwa zarejestrowanych przez oprogramowanie,
5. Zgłoszenia w ramach wsparcia technicznego będą podejmowane najpóźniej w ciągu 4 godzin od ich zgłoszenia. Usuwanie awarii będzie wykonywane nieprzerwanie do czasu zamknięcia zgłoszenia. Dopuszcza się zastosowanie ustalonej z Zamawiającym metody obejścia.

Wymagania w zakresie świadczenia usług dodatkowej asysty technicznej

1. Zamawiający wymaga zapewnienia przez Wykonawcę dodatkowych usług asysty technicznej.

2. Usługę asysty technicznej Wykonawca będzie świadczyć na każde żądanie Zamawiającego, tj. każdorazowo na podstawie pisemnego zlecenia asysty technicznej, wystawianego przez Zamawiającego, w którym Zamawiający określi rodzaj, zakres oraz termin wykonania tych usług.
3. Zakres, sposób oraz termin realizacji zostanie uzgodniony na etapie przedstawienia wymagań przez Zamawiającego i wyceny pracochłonności przez Wykonawcę, poprzedzających zlecenie. Zlecenia będą obejmować w szczególności wsparcie pracowników Zamawiającego w użytkowaniu oprogramowania zarówno techniczne jak i merytoryczne oraz implementację nowych funkcjonalności lub modyfikacji już istniejących.
4. Osoba/y realizująca Usługę dodatkowej asysty technicznej musi być ekspertem w obszarze związanym z technologią dot. dostarczonej subskrypcji oprogramowania, oraz legitymować się ważnym i aktualnym certyfikatem Producenta lub akredytowanego przez Producenta podmiotu potwierdzającym w/w wiedzę ekspercką oraz musi posiadać dostęp do bazy wiedzy tego Producenta. Równoważnym do powyższego jest świadczenie usług przez samego producenta oprogramowania, wówczas wszystkie warunki określone w niniejszym punkcie uznaje się za spełnione.

IV. MIEJSCE I TERMIN SKŁADANIA OFERT

1. Ofertę należy przesłać **do dnia 25.08.2023 r. do godz. 13.00**.
2. Oferty należy przesłać za pośrednictwem poczty elektronicznej poprzez wypełnienie załączonego formularza ofertowego na adres: ofertyIT@mrit.gov.pl,
3. Oferty dostarczone po terminie nie będą rozpatrywane.
4. Wykonawca jest zobowiązany do wskazania w ofercie terminu związania ofertą, nie krótszego niż 30 dni kalendarzowych.
5. Cena oferty powinna uwzględniać wszystkie zobowiązania, musi być podana w walucie polskiej, tj. PLN cyfrowo i słownie, wraz z należytym podatkiem VAT – jeżeli występuje.
6. Wraz z ofertą Wykonawca zobowiązany jest przekazać podpisane oświadczenie stanowiące Załącznik nr 2 do zapytania
7. Jedynym kryterium wyboru najkorzystniejszej oferty jest cena.

V. DODATKOWE INFORMACJE

1. Niniejsze zapytanie nie stanowi oferty w myśl art. 66 Kodeksu Cywilnego, jak również nie jest ogłoszeniem w rozumieniu ustawy Prawo Zamówień Publicznych.
2. Zapytanie nie jest postępowaniem o udzielenie zamówienia w rozumieniu przepisów Prawa zamówień publicznych oraz nie kształtuje zobowiązania Zamawiającego do przyjęcia którejkolwiek z ofert.
3. Zamawiający zastrzega sobie prawo do rezygnacji z zamówienia, bez wyboru którejkolwiek ze złożonych ofert.
4. Zamawiający zawiera umowy na podstawie własnych wzorów umów stosowanych w Ministerstwie Rozwoju i Technologii.