ROZDZIAŁ II – OPIS PRZEDMIOTU ZAMÓWIENIA

1. Nazwa zamówienia

Dostawa systemu udostępniającego metody MFA dla aplikacji web wraz z usługami wsparcia na okres 36 miesięcy oraz dostawą kluczy 2FA z gwarancją producenta

2. Oznaczenie przedmiotu zamówienia wg kodów CPV:

48000000-8 Pakiety oprogramowania i systemy informatyczne
35120000-1 Systemy i urządzenia nadzoru i bezpieczeństwa.
72250000-2 Usługi w zakresie konserwacji i wsparcia systemów

3. Przedmiot zamówienia

3.1. Przedmiotem zamówienia jest zapewnienie przez Wykonawcę:

3.1.1. dostawy Systemu udostępniającego mechanizmy silnego uwierzytelniania (różnymi dodatkowymi składnikami, które użytkownik może posiadać) – dalej określanego jako „**System”** i spełniającego wymagania opisane w pkt 7.1 OPZ, wraz z Instruktażem;

3.1.2. Wsparcia Technicznego Producenta dla Systemu, zgodnie z zasadami opisanymi w pkt 8 OPZ;

3.1.3. realizacji Usług Profesjonalnych, w wymiarze 500 roboczogodzin, zgodnie z zasadami opisanymi w pkt 9 OPZ;

3.1.4. dostawy 300 szt. kluczy 2FA, objętych gwarancją producenta, zgodnych z wymaganiami zdefiniowanymi w pkt. 10 OPZ;

4. Definicje

Zamawiający dokonał opisu przedmiotu zamówienia z wykorzystaniem następujących definicji:

Aktualizacje	jakiekolwiek uaktualnienia oprogramowania, dostarczonego wraz z Systemem lub kluczem 2FA, w tym dodatkowe licencje i wyższe wersje (update/upgrade), niższe wersje (downgrade), wydania uzupełniające, patche, zmiany, nowe wersje, poprawki oraz inne dostosowania, zapewniające prawidłowe korzystanie z takiego oprogramowania.
Awaria	Stan, w którym nie jest możliwe używanie przedmiotu zamówienia, w sposób zgodny z jego przeznaczeniem.
godziny robocze	godziny od 09:00 do 17:00 w dni od poniedziałku do piątku, nie będące dniami ustawowo wolnymi od pracy na terenie Rzeczypospolitej Polskiej.
dzień roboczy	oznacza dzień od poniedziałku do piątku nie będący dniem ustawowo wolnym od pracy na terenie Rzeczypospolitej Polskiej.
Instruktaż	Oznacza instruktaż stanowiskowy zapewniony przez Wykonawcę, zgodnie z wymogami zawartymi w pkt 11 OPZ.

Producent	oznacza producenta Systemu, opisanego w pkt.7
roboczogodziny	oznacza jednostkę miary czasu wykonywania usług opisanych w pkt. 3.2, obejmującą pracę jednej osoby przez godzinę, bez ograniczenia do godzin roboczych lub dnia roboczego, do której nie wlicza się czasu oraz kosztów dojazdu do lokalizacji, w której usługa jest wykonywana.
SSL/TLS	*ang.* Secure Socket Layer / Transport Layer Security oznacza protokół szyfrowania komunikacji sieciowej. (ze wsparciem co najmniej w wersji TLS 1.2 lub TLS 1.3)
Wirtualny appliance	oznacza system, dostarczany w postaci obrazu (przystosowanego do pracy na platformie wirtualizacyjnej VMWARE), umożliwiającego nieograniczone czasowo korzystanie, maintenance i wsparcie techniczne - zarówno dla oprogramowania jak i systemu operacyjnego oraz innych części składowych tego systemu.
2FA	ang. Second Factor Authentication, oznacza system klasy 2FA dostarczający mechanizm bezpiecznego dostępu do chronionego serwisu za pomocą uwierzytelniania się drugim składnikiem (który użytkownik fizycznie posiada).
Chroniony system, Chroniona aplikacja	To serwis webowy dostępny przez przeglądarkę internetową, który jest administrowany i utrzymywany przez Zamawiającego.
Tożsamość użytkownika Chronionego systemu	To opis użytkownika i jego reprezentacja w Chronionym systemie/serwisie, obejmujący atrybuty, uprawnienia i powiązania. Użytkownik w Chronionym
System	oznacza System będący przedmiotem niniejszego postepowania, dla którego wymagania zostały opisane w pkt 7 OPZ.
Umowa	oznacza umowę ws zamówienia publicznego zawartą przez Zamawiającego z Wykonawcą po zakończeniu postępowania o udzielnie zamówienia
Usługi Profesjonalne	oznacza ang. Professional Services – usługi oferowane przez Producenta, realizowane również prze podmioty działające w imieniu Producent,
Wsparcie Techniczne	oznacza świadczenia realizowane przez Producenta Systemu, obejmujące co najmniej zakres opisany w pkt 8 OPZ.

W każdym przypadku, bez względu na wielkość liter, ile razy zostaną wymienione w niniejszym dokumencie sformułowania z powyższej tabeli, należy je rozumieć w zdefiniowany wyżej sposób.

5. Termin dostawy

5.1. Zamawiający wymaga zrealizowania dostawy Systemu oraz kluczy 2FA, a także udostępnienia możliwości korzystania z usług Wsparcia Technicznego (ang. maintenance) oraz Usług Profesjonalnych, w terminie do 3 tygodni od dnia zawarcia Umowy. Wykonawca zobowiązany jest zapewnić możliwość zrealizowania Instruktażu, w okresie 5 miesięcy od dnia zawarcia Umowy.

6. Warunki dostawy

6.1. Dostawa ma zostać wykonana w Dni Robocze w godzinach roboczych, do jednej lokalizacji, na ternie m.st. Warszawy, na adres wskazany przez Zabawiającego po zawarciu Umowy.

6.2. Dostarczane oprogramowanie musi obejmować dostęp do najnowszej wersji tego oprogramowania udostępnionej przez jego Producenta. Dostarczane Klucze 2FA muszą być fabrycznie nowe, nie używane i pochodzić z oficjalnego kanału dystrybucji ich producenta.

6.3. Licencje dostarczane razem z oprogramowaniem muszą pochodzić z oficjalnego kanału dystrybucji ich Producenta. Dostarczane Klucze 2FA muszą być fabrycznie nowe, nie używane i pochodzić z oficjalnego kanału dystrybucji ich producenta.

6.4. Dostawa Systemu musi być wykonana wraz z wszystkimi licencjami i komponentami, przewidzianymi przez Producenta Systemu dla osiągniecia przez System wymogów, opisanych w pkt 7 OPZ. Dostawa kluczy 2FA musi być wykonana wraz wszystkimi licencjami i komponentami, przewidzianymi przez ich Producenta dla osiągniecia przez klucze 2FA wymogów, opisanych w pkt 10 OPZ, w tym w szczególności z przewidzianymi przez ich producenta akcesoriami tj. okablowanie, zasilacze oraz wszystkie inne komponenty, zapewniające właściwą instalację i użytkowanie – jeżeli są oferowane przez producenta razem z takimi kluczami 2FA.

6.5. Każdy przedmiot dostawy musi być dostarczony ze wszystkimi niezbędnymi do działania i zapewnienia wymaganych funkcjonalności, bezterminowymi licencjami na używanie tych funkcjonalności.

6.6. W przypadku dostawy nośników oprogramowania, okres gwarancji dla takich nośników nie będzie krótszy niż 12 miesięcy licząc od dnia podpisania przez Strony protokołu odbioru. W przypadku wystąpienia wady lub usterki nośnika oprogramowania w tym okresie, Wykonawca zobowiązany jest dostarczyć nowy nośnik, wolny od wad, w terminie 7 dni od dnia zgłoszenia wady lub usterki.

6.7. Wszystkie informatyczne nośniki danych dostarczone przez Wykonawcę, w związku z wykonywaniem Umowy, pozostaną w posiadaniu Zamawiającego w przypadku ich awarii.

6.8. Wykonawca jest zobowiązany do przekazania Zamawiającemu aktualnego zestawienia w formacie xls wszystkich dostarczonych pozycji w zakresie oprogramowania zawierającego informacje m.in. oznaczenie producenta (tzw. part numer), pełna nazwa produktu, metryka licencyjna, wersja i edycja oprogramowania, rodzaj licencji, okres obowiązywania licencji, okres obowiązywania wsparcia technicznego, poziom wsparcia technicznego, ceny jednostkowej netto, kwoty VAT oraz ceny jednostkowej brutto, zgodnie z zapisami zawartymi w SIWZ.

7. System – wymagania funkcjonalne

LP.	Opis wymagania	Parametry minimalne

1.	Ogólne	1.1. System musi dostarczać mechanizm i możliwość wprowadzenia zabezpieczenia procesu uwierzytelnienia dostępu do Chronionego systemu (dostępnego przez przeglądarkę internetową) poprzez zastosowanie dodatkowego składnika weryfikującego tożsamość użytkownika. 1.2. System musi pochodzić oraz być wspierany i rozwijany przez tego samego producenta. 1.2.1 System musi wspierać rozwiązanie klasy MFA w postaci haseł jednorazowych generowanych przez aplikacje oraz 1.2.2 fizyczne Klucze Zabezpieczające z interfejsami USB oraz wykorzystujące technologię NFC. Zamawiający wymaga dostarczenia wraz z Systemem 300 kluczy kryptograficznych M2F - z obsługą protokołu NFC (tj. to opisano w pkt. 3.4 *Specyfikacja wymagań dot. kluczy MFA*). 1.3. Podczas realizacji etapu rejestracji i weryfikacji drugiego składnika System musi komunikować się wyłącznie z infrastrukturą Zamawiającego. W procesie uwierzytelniania niedopuszczalna jest komunikacja poza infrastrukturę Zamawiającego. 1.4. System musi pracować w ramach infrastruktury zamawiającego bez konieczności dostępu do usług zlokalizowanych poza infrastrukturą zamawiającego. 1.5. Niedopuszczalne jest wywoływanie API/SDK w systemach poza infrastrukturą zamawiającego. 1.6. System 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 - wskazującej datę planowanego zakończenia sprzedaży lub wsparcia dla oferowanego produktu, przypadającą przed sierpniem 2024. Jeżeli data planowanego zakończenia przypada przed sierpniem 2024 - warunki licencyjne i wsparcie producenta muszą zapewniać aktualizację do kolejnych nowych wersji. 1.7. System musi zapewnić ochronę (za pomocą haseł jednorazowych oraz fizycznych Kluczy, o czym mowa w pkt 1.2.1 oraz 1.2.2) dla: nieograniczonej ilości Chronionych systemów/serwisów Zamawiającego co najmniej 1000 Tożsamości użytkowników Chronionych systemów. Ww. zakres został opisany z wykorzystaniem ilości Tożsamości użytkowników Chronionych systemów, ponieważ zakłada się, że ochronie przez System będą podlegać również użytkownicy aplikacji, które nie przechowują tożsamości użytkowników w centralnym repozytorium tożsamości jak np. Active Directory. Zatem System musi być niezależny od centralnego repozytorium tożsamości.

2.	Rodzaj platformy Systemu	2.1.System musi funkcjonować w formie Wirtualnego appliance pracującego w środowisku wirtualnym Zamawiającego VMWare w wersji 6 i 7. 2.2.Za Wirtualny appliance w pełni musi odpowiadać producent Systemu- w tym za poprawki bezpieczeństwa i aktualizacje.

LP.	Opis wymagania	Parametry minimalne
3.	Uwierzytelnianie i ochrona Tożsamości użytkowników Chronionych systemów	3.1. System musi mieć możliwość dołożenia drugiego składnika uwierzytelniania do każdej aplikacji WWW zamawiającego dostępnej przez przeglądarkę internetową po protokole HTTP/HTTPS niezależnie od technologii, w jakiej aplikacja została wykonana. 3.2. System musi poprawnie obsługiwać wiele standardów drugiego składnika uwierzytelniania. Na moment dostarczenia wymagana jest możliwość użycia co najmniej z: a. wykorzystywanymi przez zamawiającego urządzeniami klasy U2F/FIDO2, b. hasłami jednorazowymi generowanych przez aplikacje (np. Google Authenticator, Authy, inna aplikacja generująca kody jednorazowe zgodna z RFC 6238). 3.3. System musi poprawnie obsługiwać techologię WebAuthn zaimplementowaną w przeglądarki wykorzystywane po stronie Zamawiającego, co za tym idzie mieć możliwość dopuszczenia lokalnych autentykatorów (np. czytniki biometryczne w smartfonach/laptopach) jako drugi składnik uwierzytelniania. 3.4. System musi zapewniać możliwość jednoczesnej obsługi różnych typów drugiego składnika uwierzytelniania w ramach chronionej aplikacji. 3.5. Administrator musi mieć możliwość edycji listy typów drugiego składnika dostępnych dla użytkowników chronionej aplikacji. 3.6. System 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. 3.7. System 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. 3.8. Musi być możliwość oznaczania konkretnych adresacji sieci jako zaufanych. Użytkownicy pracujący z tak oznaczonych sieci będą dopuszczani do panelu logowania aplikacji lub jakiegokolwiek innego elementu aplikacji bez wcześniejszego uwierzytelniania się drugim składnikiem. 3.9. System musi rozpoznawać akcję wylogowania użytkownika z chronionej aplikacji i co za tym idzie, natychmiast unieważniać sesję na poziomie Systemu. 3.10. 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. 3.11. Uwierzytelnienie musi być wydawane dla konkretnego adresu IP - przy zmianie adresu IP użytkownik musi być poproszony o ponowne uwierzytelnienie się. 3.12. System musi mieć możliwość modyfikacji nagłówków HTTP związanych z bezpieczeństwem aplikacji, w szczególności:

LP.	Opis wymagania	Parametry minimalne
		a. możliwość nadpisania/modyfikowania Content-Security-Policy bez zmian w chronionej aplikacji ani w serwerach HTTP serwujących chronioną aplikację, b. możliwość dodania/nadpisania nagłówka HSTS bez zmian w chronionej aplikacji ani w serwerach HTTP serwujących chronioną aplikację. **Awaryjny dostęp do chronionych aplikacji:** 3.13. System musi umożliwiać generowanie jednorazowych kodów dla użytkowników, którzy z losowych powodów nie mogą uwierzytelnić się zarejestrowanym drugim składnikiem. 3.14. Musi być możliwość konfiguracji długości kodu jednorazowego dla chronionej aplikacji. 3.15. Musi być możliwość konfiguracji ilości nieudanych prób, po których kod jednorazowy będzie automatycznie unieważniany. 3.16. Musi być możliwość definiowania każdorazowo czasu ważności kodu jednorazowego wydawanego użytkownikowi. **Warunkowe zaufanie dla środowiska użytkownika:** 3.17. System musi umożliwiać włączenie opcji zaufania przeglądarce na wskazanym urządzeniu. Po zaufaniu przeglądarce użytkownik nie będzie proszony o uwierzytelnienie się drugim składnikiem przez określony czas. 3.18. Możliwość zaufania przeglądarce musi być konfigurowalna dla każdej chronionej aplikacji. 3.19. Czas, na jaki przeglądarka ma zostać oznaczona jako zaufana, musi być konfigurowalny przez administratora Systemu. 3.20. Musi istnieć możliwość definiowania różnego czasu zaufania przeglądarce dla różnych Chronionych aplikacji.
4.	Redundancja i dostępność	4.1. System musi pracować w modelu active/active. Dostawca musi zapewnić odpowiednie licencje i wsparcie pozwalające na w/w architekturę. 4.2. Dostarczone rozwiązanie musi umożliwiać uruchomienie minimum 2 węzłów Systemu. 4.3. System musi umożliwiać pracę w co najmniej 2-węzłowym klastrze active-active. 4.4. System musi umożliwiać pracę pojedynczego węzła przy przepustowości minimum 500Mbps.
5.	Protokół IP	5.1. System musi umożliwiać ochronę (w zakresie uwierzytelniania) systemów wykorzystujących technologię IPv4.
6.	Monitoring i dziennik zdarzeń	6.1. System musi zapewniać możliwość wysyłania zdarzeń bezpieczeństwa (audyt i zarejestrowane zdarzenia bezpieczeństwa) w postaci logów do zewnętrznych systemów klasy SIEM. 6.2. System musi mieć wewnętrzne mechanizmy do monitorowania wydajności i dostępności poszczególnych jego zasobów wraz z możliwością powiadamiania zewn. systemów monitorujących stan dostępności lub administratorów o wystąpieniu problemów. 6.3. System musi posiadać moduł logowania zdarzeń.

LP.	Opis wymagania	Parametry minimalne
		6.4. Moduł logowania zdarzeń musi mieć możliwość wysyłania logów do zewnętrznego serwera syslog. 6.5. 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. 6.6. 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. 6.7. Moduł logowania zdarzeń musi logować zdarzenia zachodzące w ramach konfiguracji Systemu, w szczególności: a. rejestracja nowej aplikacji, b. dodanie/usunięcie użytkownika panelu administracyjnego, c. wszystkie zmiany w ramach konfiguracji Systemu, d. logowanie do panelu administracyjnego/API.
7.	Zarządzanie	7.1. System musi umożliwiać zarządzanie za pomocą interfejsu graficznego. W przypadku użycia technologii Java wymagane jest dostarczenie odpowiednich licencji, aby móc legalnie użytkować tą technologię. 7.2. System musi wspierać połączenia bezpiecznym kanałem szyfrowanym z wykorzystaniem SSL/TLS od wersji 1.2 wzwyż. 7.3. Musi umożliwiać różnicowanie dostępu dla różnych administratorów. 7.4. Musi pozwalać na zdefiniowanie min. 10 administratorów, mogących pracować równolegle. 7.5. System musi umożliwiać użytkownikom chronionej aplikacji zarządzanie przypisanymi do użytkownika dodatkowymi składnikami uwierzytelniania. Co najmniej: przeglądanie, dodawanie i usuwanie. 7.6. Interfejs do zarządzania dodatkowymi składnikami uwierzytelniania musi być dostępny dla użytkownika w kontekście interfejsu chronionej aplikacji po zalogowaniu się do niej. 7.7. Zarządzanie konfiguracją musi być możliwe za pomocą dedykowanego panelu administracyjnego i poprzez API. 7.8. Panel administracyjny musi umożliwiać granulację uprawnień. 7.9. Granulacja uprawnień na poziomie panelu administracyjnego powinna umożliwiać dowolne przypisywanie użytkownikowi administracyjnemu ról, co najmniej: a. administratora Systemu (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,

LP.	Opis wymagania	Parametry minimalne
		dostęp do logów niezbędnych do rozwiązywania problemów użytkownika końcowego chronionej aplikacji). 7.10. Wszystkie akcje dostępne poprzez panel administracyjny muszą być dostępne poprzez API. 7.10. API musi pozwalać na automatyzację podstawowych zadań administracyjnych (np. wykonywanie kopii zapasowej konfiguracji Systemu). 7.11. API musi być chronione tymi samymi poświadczeniami co panel administracyjny
8.	Implementacja Systemu	8.1. System 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). 8.2. Wdrożenie Systemu nie może wymagać zmian w architekturze technicznej w chronionych aplikacjach. 8.3. Wdrożenie Systemu nie może wymagać integracji z API Chronionych aplikacji. 8.4. Wdrożenie Systemu nie może wymagać integracji z usługami dostarczającymi tożsamość. 8.5. Dostarczone rozwiązanie nie może wymagać obsługi standardów SAML/OpenID/OAuth od chronionych aplikacji. 8.6. Nie dopuszcza się, aby System przechowywał hasła użytkowników do Chronionych aplikacji w jakiejkolwiek formie.
9.	**Polityki dostępu dla użytkowników Chronionych aplikacji:**	9.1. System musi mieć możliwość stosowania różnych polityk dotyczących logowania, w tymco 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 System nie może pozwolić na zalogowanie się użytkownika, który nie zarejestrował drugiego składnika uwierzytelniania, c. rejestracja wybiórcza - System wymaga zarejestrowania i używania drugiego składnika uwierzytelniania dla wybranych, nazwanych użytkowników (np. dla użytkowników o podwyższonych uprawnieniach w chronionej aplikacji), d. ograniczanie dostępu - System dopuszcza rejestrację drugiego składnika i logowanie do Chronionej aplikacji tylko wybranym, nazwanym użytkownikom.

LP.	Opis wymagania	Parametry minimalne
10.	Dodatkowe wymagania	*10.1. 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[1].* *10.2. Rozwiązanie powinno wspierać aplikacje z własnymi bazami użytkowników i je wykorzystywać wyłącznie w pierwszym kroku procesu uwierzytelniania (w momencie podawania nazwy użytkownika i hasła)[2].* *10.3. 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 Systemu. 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 Systemu. 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)[3].* 10.4. System musi umożliwiać administratorowi systemu dopuszczenie kluczy kryptograficznych do użytku na podstawie zawartości certyfikatu atestacyjnego danego klucza kryptograficznego. Dopuszczenie o którym mowa w powyżej odbywa się będzie przez budowanie przez administratora systemu kryteriów kwalifikujących. Przykładem dopuszczenia może być określona seria kluczy albo producenta.

8. Wsparcie Techniczne - wymagania minimalne

8.1. Wykonawca zobowiązany jest zapewnić Wsparcie Techniczne (ang. maintenance) Producenta lub autoryzowanego podmiotu współpracującego z Producentem w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego Producenta lub poziomie niższym, o nie więcej niż jeden stopień, działającego w imieniu tego Producenta, dla Systemu, przez okres 36 miesięcy, od dnia odbioru Systemu.

8.2. Zapewnienie usługi wsparcia, obejmuje nieograniczony dostęp do wszystkich udostępnionych przez Producenta Aktualizacji, poprawek, komunikatów, subskrypcji, dokumentacji technicznej, baz wiedzy, instrumentów zgłaszania błędów.

8.3. Dostęp do uaktualnień sygnatur/reguł i poprawek i Aktualizacji licencji/oprogramowania będzie realizowany przez konto udostępnione przez Producenta wraz z niezbędnymi danymi logowania, umożliwiające samodzielne (bezpośrednio u Producenta) pobieranie uaktualnień sygnatur/reguł oraz

[1] Stanowi kryterium oceny ofert
[2] Stanowi kryterium oceny ofert
[3] Stanowi kryterium oceny ofert

poprawek i aktualizacji oprogramowania w ramach posiadanej licencji oraz umożliwiające zakładanie zgłoszeń serwisowych w trybie 24/7/365.

8.4. Zgłoszenia serwisowe 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 zaakceptowanego przez Zamawiającego obejścia.

9. Usługi Profesjonalne[4]

9.1. Zamawiający wymaga zapewnienia przez Wykonawcę Usług Profesjonalnych świadczonych bezpośrednio przez Producenta lub autoryzowany podmiot współpracujący z Producentem w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej Producenta lub poziomie niższym, o nie więcej niż jeden stopień, działający w imieniu tego Producenta - w wymiarze łącznie 500 roboczogodzin, przez okres 36 miesięcy od dnia odbioru ilościowego Systemu, zgodnie z Umową.

9.2. Osoba/y realizująca Usługę Profesjonalną musi być ekspertem w obszarze związanym z technologią dot. **Systemu** 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.

9.3. Zakres przedmiotowy Usług Profesjonalnych będzie obejmować m.in.:

9.3.1. opracowanie i dostarczenie projektu wdrożenia Systemu oraz związanej z tym wdrożeniem dokumentacji powykonawczej, a także przeniesienie majątkowych praw autorskich, do utworów wytworzonych w toku wykonywania Usług Profesjonalnych (nie dotyczy nowego kodu Systemu i jego wersji wytwarzanych w czasie utrzymania i wsparcia systemu dla Zamawiającego),

9.3.2. opracowanie i dostarczenie procedury postępowania w razie wystąpienia błędów lub Awarii wraz z formularzami zgłoszeniowymi i osobami kontaktowymi (nr tel., e-mail) do konsultacji rozwiązywania zaistniałych problemów,

9.3.3. wsparcie we wdrożeniu i konfiguracji Systemu,

9.3.4. konsultacje dot. utrzymania, eksploatowania oraz analizy zdarzeń bezpieczeństwa zarejestrowanych przez System ,

9.3.5. przygotowanie i przeprowadzenie instruktażu w zakresie korzystania z Systemu, w taki sposób, aby każda z osób uczestniczących w instruktażu posiadała wiedzę i umiejętności potrzebne do prawidłowej obsługi i samodzielnej konfiguracji Systemu, z wykorzystaniem jego wszystkich funkcjonalności – niezależnie od zobowiązania do zapewnienia Instruktażu zgodnie z pkt 11 OPZ. Zamawiający będzie wymagał przeprowadzenia takiego instruktażu przez co najmniej jedną osobę, która w okresie dwóch lat przed realizacją instruktażu ukończyła szkolenie oferowane przez producenta Systemu, w zakresie objętym instruktażem oraz legitymuje się certyfikatem potwierdzającym ukończenie takiego szkolenia.

9.4. Zamawiający wymaga zapewnienia realizacji Usług Profesjonalnych, na podstawie zleceń przekazywanych przez personel Zamawiającego, wskazany w zawartej z wykonawcą Umowie, wskazujących przedmiot zamawianych usług, a Wykonawca będzie zobowiązany zapewnić rozpoczęcie świadczenia takich usług nie później niż w terminie 3 dni roboczych od dnia przekazania Wykonawcy zlecenia.

9.5. Zamawiający wymaga realizowania Usług Profesjonalnych zarówno w godzinach roboczych jak i poza godzinami roboczymi – w terminach i zakresie uzgodnionych z Wykonawcą, przed udzieleniem zlecenia.

[4] Cały zakres tej usługi objęty jest opcją i Zamawiający nie jest zobowiązany do zlecenia jakiejkolwiek ilości usług jako Usług Profesjonalnych. Usługi Profesjonalne są usługą realizowaną wyłącznie na zlecenie Zamawiającego, jako opcja, w rozumieniu przepisu art. 441 Ustawy Pzp.

10. Klucze 2FA

10.1. Zamówienie obejmuje jednorazową dostawę 300 szt. Kluczy 2FA : YubiKey 5 NFC FIDO [model obsługujący technologię NFC] z USB typ A lub równoważnych, spełniających następujące kryteria oceny równoważności:

10.1.1. Zgodność z otwartym standardem uwierzytelniania U2F, który umożliwia urządzeniom kluczy na bezpieczne uzyskiwanie dostępu do dowolnej liczby usług sieciowych.

10.1.2. Obsługa silnego mechanizm uwierzytelniania Yubi OTP lub równoważny.

10.1.3. Obsługa funkcjon.alności OATH-TOPT (ang. Time-Based One-Time Password Algorithm) - wygenerowane hasło (PIN) oparte na funkcji czasu oraz OATH-HOPT (ang. Hmac-Based One-Time Password Algorithm), gdzie zamiast funkcji czasu używany jest licznik uwierzytelniania.

10.1.4. Obsługa funkcjonalności PIV (ang. Personal Identity and Verification Card) - Umożliwia podpisanie i deszyfrowanie podpisów RSA lub ECC przy użyciu prywatnego klucza.

10.1.5. Zgodność z CCID - Protokół interfejsu karty chipowej (protokół karty chipowej) to protokół USB umożliwiający podłączenie karty inteligentnej do komputera przy użyciu standardowego interfejsu USB.

10.1.6. Obsługa technologii NFC. Operacja wydania poświadczenia musi następować w wyniku dotknięcia płytki pojemnościowej wbudowanej w klucz kryptograficzny lub poprzez zbliżenie klucza do anteny NFC

10.1.7. Klucze muszą pasować do gniazd USB typu A .

10.1.8. Klucze musza być zgodne z wymogiem wskazanym w punkcie 10.4. tabeli zawartej w punkcie 7 OPZ

10.2. Zamawiający wymaga objęcia dostarczonych kluczy 2FA gwarancją producenta, zgodną z postanowieniami wskazanymi w Umowie. Gwarancja musi obejmować co najmniej:

10.2.1. odpowiedzialność producenta, co najmniej za wady powstałe z przyczyn tkwiących w dostarczonych kluczach 2FA, przez okres co najmniej 24 miesięcy, od dnia ich wydania Zamawiającemu;

10.2.2. zobowiązanie do usunięcia Awarii klucza 2FA przez producenta (lub jego sieć usług serwisowych) niezwłocznie, ale nie później niż w terminie czternastu dni, licząc od dnia dostarczenia przedmiotu objętego Awarią, do punktu wskazanego przez producenta.

10.3. Zamawiający wymaga objęcia dostarczonych kluczy 2FA objętych wsparciem technicznym ich producenta (ang. support), przez okres co najmniej 24 miesięcy od dnia ich wydania Zamawiającemu, pod warunkiem ich udostępniania przez producenta kluczy 2FA, obejmującym co najmniej:

10.3.1. możliwość pobierania Aktualizacji,

10.3.2. możliwość korzystania z bazy wiedzy i forów konsultacyjnych,

10.3.3. możliwość korzystania z innych świadczeń – oferowanych przez producenta kluczy 2FA razem z samymi kluczami 2FA.

11. Instruktaż

11.1. Zamawiający wymaga zapewnienia Instruktażu dla 5 osób, w terminie pięciu miesięcy od dnia zawarcia umowy.

11.2. Instruktaż musi obejmować zakres dot. konfiguracji i administracji Systemem, trwające min. 2 Dni Robocze – dla każdej z 5 osób wskazanych przez Zamawiającego. Wykonawca zobowiązany jest zapewnić możliwość przeprowadzenia dwóch dni Instruktażu, dla grupy do 5 z takich osób w jednym terminie, w każdym z pośród pięciu miesięcy, według wyboru Zamawiającego.

11.3. Zamawiający będzie uprawniony do wymagania realizacji Instruktażu z możliwością aktywnego udziału uczestników szkolenia – w języku polskim.

11.4. Zamawiający dopuszcza możliwość zapewnienia Instruktażu poprzez ddostarczenie tzw. voucherów uprawniających do uczestniczenia w instruktażu organizowanym przez producenta Systemu, (dalej określanego jako „Producent") lub autoryzowany przez Producenta podmiot – z zastrzeżeniem pozostałych wymogów dotyczących Instruktażu, w szczególności możliwości wyboru jednego terminu w każdym z 5 miesięcy od dnia zawarcia Umowy.

11.5. Instruktaż może zostać przeprowadzony w częściach wyżej wskazanych w pkt. 11.2 (zależnie od potrzeb zamawiającego), w ośrodku szkoleniowym w Warszawie lub online - pod warunkiem zapewnienia możliwości aktywnego udziału w Instruktażu on-line, w tym zadawania pytań i uzyskiwania odpowiedzi w czasie szkolenia.

12. Ogólne zasady oceny równoważności

12.1. Przedmiot zamówienia został opisany przez odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, a Zamawiający dopuszcza rozwiązania równoważne opisywanym i takim odniesieniom towarzyszą wyrazy "lub równoważne".

12.2. W przypadku gdy opis przedmiotu zamówienia odnosi się do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 Pzp., Zamawiający nie odrzuci oferty tylko dlatego, że oferowane dostawy lub usługi nie są zgodne z normami, ocenami technicznymi, specyfikacjami technicznymi i systemami referencji technicznych, do których opis przedmiotu zamówienia się odnosi, pod warunkiem że wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, o których mowa w art. 104-107 Pzp., że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia.

12.3. W przypadku gdy opis przedmiotu zamówienia odnosi się do wymagań dotyczących wydajności lub funkcjonalności, o których mowa w art. 101 ust. 1 pkt 1 Pzp., zamawiający nie odrzuci oferty zgodnej z Polską Normą przenoszącą normę europejską, normami innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszącymi normy europejskie, z europejską oceną techniczną, ze wspólną specyfikacją techniczną, z normą międzynarodową lub z systemem referencji technicznych ustanowionym przez europejski organ normalizacyjny, jeżeli te normy, oceny techniczne, specyfikacje i systemy referencji technicznych dotyczą wymagań dotyczących wydajności lub funkcjonalności określonych przez zamawiającego, pod warunkiem że wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, o których mowa w art. 104-107, że dostawa lub usługa, spełniają wymagania dotyczące wydajności lub funkcjonalności określone przez zamawiającego.

12.4. W przypadku, gdy zaoferowane przez Wykonawcę rozwiązanie równoważne (dotyczy równoważności we wszystkich wskazanych powyżej przypadkach) nie będzie poprawnie współpracować z oprogramowaniem lub sprzętem Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu infrastruktury Zamawiającego, Wykonawca podejmie na własny koszt wszelkie niezbędne działania celem przywrócenia sprawnego działania infrastruktury, w tym dokona ewentualnych niezbędnych modyfikacji po odinstalowaniu rozwiązania.

12.5. Zastosowanie rozwiązania równoważnego nie może wymagać żadnych nakładów, których nie wymagałoby również zastosowanie rozwiązań opisanych, jako rozwiązania referencyjne, po stronie Zamawiającego, celem dostosowania do niego aktualnie posiadanej przez Zamawiającego infrastruktury ani w warstwie fizycznej ani w warstwie oprogramowania.

12.6. Wykonawca zobowiązany jest podać w ofercie co najmniej nazwę producenta, nazwę oferowanych kluch 2FA, identyfikator takich kluczy 2FA nadawany przez jego producenta, rodzaj licencji (według oznaczenia producenta), w sposób umożliwiający Zamawiającemu jednoznaczną identyfikację i

weryfikację zaoferowanego klucza 2Fa oraz udowodnić, że oferowane rozwiązanie spełnia wskazane przez Zamawiającego kryteria stosowane w celu oceny równoważności.

12.7. Zamawiający nie dopuszcza dostarczenia licencji dla produktów równoważnych w formie upgradu, licencji czasowej, OEM, chyba że Zamawiający określił taki warunek w opisie oprogramowania.

12.8. Zamawiający nie dopuszcza zaoferowania subskrybcji licencyjnej opartej o rozwiązania chmurowe z wyłączeniem sytuacji, w którym Zamawiający określił taki warunek w opisie oprogramowania.

12.9. W przypadku błędnego działania środowiska lub wykrytych niezgodności pod kątem spełnienia warunków OPZ po instalacji oprogramowania równoważnego Zamawiający ma prawo odstąpić od umowy.