

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA (SOPZ)

Nazwa: „Usługa polegająca na świadczeniu usług zaufania – tworzenia i wydawania kwalifikowanych certyfikatów podpisu elektronicznego oraz certyfikatów niekwalifikowanych wraz ze świadczeniem usług komplementarnych dla Urzędu Marszałkowskiego Województwa Mazowieckiego w Warszawie”.

1. SŁOWNIK POJĘĆ

Ustawa - Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2021 poz. 1797 t.j.)

eIDAS- Rozporządzenie Parlamentu Europejskiego i Rady UE nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające Dyrektywę Parlamentu Europejskiego i Rady UE w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (eIDAS) 1999/93/WE.

Certyfikat podpisu elektronicznego – poświadczenie elektroniczne, które przyporządkowuje dane służące do walidacji podpisu elektronicznego do osoby fizycznej i potwierdza co najmniej imię i nazwisko lub pseudonim tej osoby.

Certyfikat kwalifikowany– kwalifikowany certyfikat podpisu elektronicznego w rozumieniu **Ustawy**.

Podpis elektroniczny - dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej i które użyte są przez podpisującego, jako podpis.

Kwalifikowany podpis elektroniczny - zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego.

Kwalifikowany Dostawca Usług Zaufania - dostawca usług zaufania, który świadczy przynajmniej jedną usługę zaufania i któremu status kwalifikowany nadał organ nadzoru. Podmiot ten nazywany będzie Centrum Certyfikacji.

Usługi zaufania - Usługa elektroniczna obejmująca:

- a) tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; lub
- b) tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych; lub
- c) konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami.

Znakowanie czasem - usługa polegająca na dołączaniu do danych w postaci elektronicznej logicznie powiązanych z danymi opatrzonymi podpisem lub poświadczeniem elektronicznym, oznaczenia czasu w chwili wykonania tej usługi oraz poświadczenia elektronicznego tak powstałych danych przez podmiot świadczący tę usługę.

Polityka Certyfikacji - szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki bezpieczeństwa tworzenia i stosowania certyfikatów.

Dni robocze – od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.

2. PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest świadczenie usług zaufania w zakresie:

- 1) wydawania certyfikatów kwalifikowanych dla wskazanych pracowników Zamawiającego i świadczenia usług zaufania związanych z ich obsługą;
- 2) weryfikacji tożsamości pracowników Zamawiającego, dla których wydawane są certyfikaty, w tym: zapewnienie nieodpłatnego dostępu do autoryzowanego punktu weryfikacji tożsamości zlokalizowanego na terenie Warszawy lub świadczenie usługi grupowej weryfikacji tożsamości w siedzibie Zamawiającego lub świadczenie usługi weryfikacji tożsamości w siedzibie Zamawiającego dla pracowników VIP lub zdalna weryfikacja tożsamości z wykorzystaniem dostępnych środków komunikacji elektronicznej;
- 3) odnawiania certyfikatów kwalifikowanych;
- 4) dostawy zestawów do składania kwalifikowanego podpisu elektronicznego z certyfikatem kwalifikowalnym podpisu elektronicznego, z kartą mini i czytnikiem mini, spełniających wymagania kwalifikowanego urządzenia do składania kwalifikowanego podpisu elektronicznego;
- 5) zagwarantowanie pakietu minimum 5 000 kwalifikowanych elektronicznych znaczników czasu miesięcznie dla każdego wydanego lub odnowionego certyfikatu;
- 6) wydania lub odnowienia certyfikatów niekwalifikowanych Certum S/MIME Sponsor, lub równoważnych zgodnie z przepisami zawartymi w **Ustawie** i **eIDAS**.

Świadczenie usług zaufania, o których mowa w pkt 1 obejmuje w szczególności:

- wydawanie certyfikatów kwalifikowanych dla wskazanych pracowników Zamawiającego,
- zawieszenie certyfikatu kwalifikowanego,
- unieważnianie certyfikatów na wniosek Zamawiającego,
- publikowanie list zawieszonych i unieważnionych certyfikatów,
- świadczenie wsparcia technicznego zgodnie z Polityką Certyfikacji Wykonawcy.

Zamawiający oświadcza, że w ramach zamówienia podstawowego:

- 1) **wydanie** certyfikatów kwalifikowanych **na okres 1 roku** będzie uzależnione od aktualnych potrzeb Zamawiającego (wg oszacowania: **do 100 sztuk**), przy czym rozliczeniu będzie podlegać faktycznie wydana ilość;
- 2) **odnowienie** certyfikatów kwalifikowanych **na okres 1 roku** będzie uzależnione od aktualnych potrzeb Zamawiającego (wg oszacowania: **do 300 sztuk**), przy czym rozliczeniu będzie podlegać faktycznie odnowiona ilość;

- 3) **wydanie** certyfikatów kwalifikowanych **na okres 3 lat** będzie uzależnione od aktualnych potrzeb Zamawiającego (wg oszacowania: **do 3 sztuk**), przy czym rozliczeniu będzie podlegać faktycznie wydana ilość;
- 4) dokona **odnowienia 3** certyfikatów kwalifikowanych **na okres 3 lat**;
- 5) **wydanie** certyfikatów niekwalifikowanych **na okres 1 roku** będzie uzależnione od aktualnych potrzeb Zamawiającego (wg oszacowania: **do 300 sztuk**), przy czym rozliczeniu będzie podlegać faktycznie wydana ilość;
- 6) dokona **odnowienia 1600** sztuk certyfikatów niekwalifikowanych **na okres 1 roku**.

Zamówienie uzupełniające:

Zamawiający może zwiększyć ilość certyfikatów w okresie obowiązywania umowy na podstawie odrębnego zlecenia uzupełniającego, a Wykonawca nie może odmówić wykonania tej usług. Wykonawca zagwarantuje utrzymanie ceny za dodatkowe certyfikaty w wysokości identycznej, jak w zamówieniu podstawowym.

Wynagrodzenie za dodatkowe zlecenie zostanie rozliczone odrębnie.

Zamawiający zastrzega, że łączna wartość zamówienia podstawowego oraz zamówienia uzupełniającego nie przekroczy wartości 130.000,00 zł netto.

3. OPIS REALIZACJI ZAMÓWIENIA

A. Warunki dostawy zestawów do kwalifikowanych podpisów elektronicznych, realizacji usługi weryfikacji tożsamości oraz usługi wystawienia certyfikatu kwalifikowanego

- 1) Zamawiający zastrzega możliwość składania zamówienia na zestawy do podpisu kwalifikowanego sukcesywnie, zgodnie z bieżącymi potrzebami. Zestawy zostaną dostarczone do siedziby zamawiającego w terminie nie dłuższym niż pięć dni roboczych.
- 2) Zamawiający przekaze Wykonawcy niezbędne dane oraz dokumenty do przeprowadzenia procesu wystawienia certyfikatu kwalifikowanego zgodnie z procedurami i Polityką Certyfikacji Wykonawcy najpóźniej w dniu realizacji usługi weryfikacji tożsamości konkretnego pracownika lub grupy pracowników.
- 3) Wykonawca dokona weryfikacji tożsamości pracowników Zamawiającego, dla których wydawane są certyfikaty w jednym z wybranych sposobów: w autoryzowanym punkcie weryfikacji tożsamości zlokalizowanego na terenie Warszawy lub formie usługi grupowej weryfikacji tożsamości w siedzibie Zamawiającego lub w formie usługi weryfikacji tożsamości w siedzibie Zamawiającego dla pracowników VIP lub w formie zdalnej weryfikacji tożsamości z wykorzystaniem dostępnych środków komunikacji elektronicznej..
- 4) Od momentu otrzymania zgłoszenia od Zamawiającego, Wykonawca w terminie nie dłuższym niż dwóch dni roboczych skontaktuje się z Zamawiającym w celu ustalenia terminu przeprowadzenia czynności weryfikacji tożsamości wskazanych osób w jednej z form wskazanych w pkt. 3).
- 5) W przypadku osób wskazanych do weryfikacji tożsamości w siedzibie Zamawiającego lub zdalnej weryfikacji Wykonawca w umówionym terminie oraz miejscu przeprowadzi usługę weryfikacji tożsamości.

- 6) Wykonawca po przeprowadzanej weryfikacji tożsamości pracowników Zamawiającego przeprowadzi proces wystawienia certyfikatów kwalifikowanych pozwalających na składanie kwalifikowanego podpisu elektronicznego.
- 7) Wykonawca zobowiązany jest do zapewnienia możliwości weryfikacji tożsamości w punkcie znajdującym się na terenie Warszawy.
- 8) Wykonawca nie będzie pobierał od subskrybenta żadnych dodatkowych opłat za przeprowadzenie weryfikacji tożsamości.
- 9) Wykonawca wystawi certyfikat kwalifikowany ważny przez okres 1 roku.

Certyfikat kwalifikowany do składania kwalifikowanego podpisu elektronicznego powinien:

- 1) Posiadać okres ważności 1 rok lub 3 lata, w zależności od potrzeb Zamawiającego,
- 2) Upoważniać do wykorzystania pakietu co najmniej 5 000 sztuk kwalifikowanych znaczników czasu miesięcznie w okresie ważności certyfikatu kwalifikowanego. Znaczniki będą pobierane przez dostarczone oprogramowanie do składania podpisu elektronicznego, gdy tylko zostanie włączona taka funkcja. Wszelkie niezbędne dane konfiguracyjne oraz klucze dostępu do tej usługi zostaną dostarczone,
- 3) Spełniać wymagania stawiane w **Ustawie i eIDAS**,
- 4) Spełniać wymagania aktów wykonawczych wydanych do **Ustawy**,
- 5) Wykorzystywać algorytm obowiązujący dla chwili wystawienia, SHA2 lub lepszy, o minimalnej długości klucza 2048 bit,
- 6) Być automatycznie rozpoznawany jako zaufany w programach **ADOBE**.
- 7) Współpracować m.in. z usługami:
 - a) Platformy ePUAP: <https://epuap.gov.pl>;
 - b) Platformy Płatnik: <https://pue.zus.pl/platnik>;
 - c) Platformy EZD RP (System Elektronicznego Zarządzania Dokumentami RP; wcześniej jako EZD Podlaskiego Urzędu Wojewódzkiego);

B. Warunki świadczenia usługi odnowienia certyfikatu kwalifikowanego

- 1) Wykonawca przeprowadzi proces odnowienia certyfikatów kwalifikowanych pozwalających na składanie kwalifikowanego podpisu elektronicznego na kolejny okres ważności 1 roku lub 3 lat na zlecenie Zamawiającego.
- 2) Zamawiający wraz ze zleceniem, o którym mowa w pkt 1, przekaże Wykonawcy niezbędne dane do przeprowadzenia procesu odnowienia ważności certyfikatu kwalifikowanego zgodnie z procedurami i Polityką Certyfikacji Wykonawcy.
- 3) Odnowianie certyfikatów kwalifikowanych będzie realizowane w ramach dostępnych zasobów na karcie kryptograficznej CERTUM, będącej w posiadaniu właściciela certyfikatu podpisu elektronicznego.

- 4) Odnowieniu będą podlegały certyfikaty kwalifikowane CERTUM.
- 5) Odnowienie ważnego certyfikatu kwalifikowanego nie może powodować konieczności ponownej weryfikacji tożsamości pracownika, w szczególności potrzeby osobistego udawania się do punktu weryfikacji tożsamości.
- 6) Zamawiający informuje, że posiada karty kryptograficzne mini (wielkość karty SIM) - StarCos® 3.5 obsługiwane przez czytniki kart - ACS ACR39T. W przypadku konieczności wymiany karty kryptograficznej w celu przeprowadzenia odnowienia certyfikatu – dostarczenie nowej karty leży po stronie Wykonawcy. Wykonawca dostarczy kartę kryptograficzną w takim samym formacie jak karta wymieniana, kompatybilną z posiadanym przez użytkownika czytnikiem kart. W procesie odnawiania certyfikatu na nowej karcie Zamawiający dopuszcza weryfikację tożsamości pracownika przez uprawnionych pracowników Wykonawcy w siedzibie Zamawiającego lub przez pracownika Zamawiającego na warunkach określonych lit. A. Od momentu otrzymania zlecenia od Zamawiającego, Wykonawca w terminie nie dłuższym niż dwóch dni roboczych skontaktuje się z Zamawiającym w celu ustalenia terminu przeprowadzenia czynności weryfikacji tożsamości wskazanych osób w siedzibie Zamawiającego w Warszawie. Wykonawca nie będzie pobierał od subskrybenta żadnych dodatkowych opłat za przeprowadzenie weryfikacji tożsamości.
- 7) Zapewnienie niezbędnego do przeprowadzenia odnowienia certyfikatu, specjalistycznego oprogramowania komputerowego leży po stronie Wykonawcy.

C. Warunki dostarczenia zestawów do składania kwalifikowanych podpisów elektronicznych

- 1) Wykonawca dostarczy do siedziby Zamawiającego zestawy do składania kwalifikowanych podpisów elektronicznych na zlecenie Zamawiającego.
- 2) Zamawiający wraz ze zleceniem, o którym mowa w pkt 1 przekaże Wykonawcy niezbędne dane do przeprowadzenia procesu wystawienia certyfikatu kwalifikowanego zgodnie z procedurami i Polityką Certyfikacji Wykonawcy będącego elementem składowym zestawu.
- 3) Proces wystawienia certyfikatów kwalifikowanych zostanie zrealizowany zgodnie z wymaganiami lit. A.

D. Zestawy do składania kwalifikowanego podpisu elektronicznego powinny zawierać:

- 1) Certyfikat kwalifikowany do składania kwalifikowanego podpisu elektronicznego zgodny z wymaganiami wskazanymi w **Ustawie** o okresie ważności 1 rok lub 3 lata.
- 2) Kartę kryptograficzną (mini) zgodną z wymaganiami **Ustawy** oraz aktów wykonawczych do niej i **eIDAS** stanowiącą kwalifikowane urządzenie do składania podpisu elektronicznego.
- 3) Czytnik kart kryptograficznych (mini) o poniższych parametrach:
 - a) złącze USB kompatybilne z USB 1.1, 2.0, 3.0 i nowszymi.
 - b) niewymagający dodatkowego źródła zasilania (poza portem USB).
 - c) kompaktowy, o zwartej konstrukcji niewymagającej używania dodatkowych przewodów do podłączenia do standardowego portu USB komputera.
 - d) estetycznie wykonany, przystosowany do przenoszenia wraz z kartą kryptograficzną mini.

- e) obsługujący w pełnym zakresie dostarczone karty kryptograficzne, lub posiadane przez Zamawiającego w przypadku odnawiania certyfikatów z użyciem tych kart.
 - f) Kompatybilny z systemami operacyjnymi MS Windows: 10, 11. Dostępne sterowniki dla systemów z rodziny Linux oraz Mac OS.
 - g) kompatybilny z oprogramowaniem służącym do składania i weryfikacji podpisów elektronicznych, kwalifikowanych podpisów elektronicznych oraz zarządzania certyfikatami na karcie kryptograficznej, dostarczonym/udostępnionym przez Wykonawcę.
- 4) Oprogramowanie do składania i weryfikacji podpisów elektronicznych, w tym podpisów elektronicznych weryfikowanych z wykorzystaniem certyfikatów kwalifikowanych oraz obsługi kart kryptograficznych spełniających co najmniej poniższe wymagania:
- a) dostarczone przez Wykonawcę oprogramowanie do weryfikacji podpisów elektronicznych i kwalifikowanych podpisów elektronicznych powinno być bezpłatne w użytkowaniu i ogólnodostępne dla odbiorców dokumentów podpisanych podpisem wystawianym przy użyciu certyfikatów dostarczonych przez Wykonawcę oraz pozwalać na:
 - weryfikację podpisu elektronicznego złożonego przy użyciu certyfikatu kwalifikowanego wystawionego przez jedno z dostępnych w Polsce kwalifikowanych Centrów Certyfikacji.
 - weryfikację znacznika czasu bez względu na dostawcę tej usługi po stronie osoby podpisującej.
 - zgodne z eIDAS, w tym obsługujące algorytm funkcji skrótu SHA2 oraz różne długości kluczy kryptograficznych.
 - b) oprogramowanie do składania podpisu elektronicznego powinno co najmniej umożliwiać realizację następujących funkcjonalności:
 - złożenie podpisu elektronicznego,
 - złożenie kontrasygnaty dla podpisanego dokumentu podpisem elektronicznym,
 - obsługę wielopodpisu,
 - znakowania czasem.
 - składanie podpisów elektronicznych wewnętrznych oraz zewnętrznych w formacie XAdES i podpisów wewnętrznych w formacie PAdES.
 - składanie podpisu elektronicznego wraz z rodzajem zobowiązania „Proof of approval”, oraz bez zobowiązania.
 - podpisywanie zarówno pojedynczych plików jak też wielu plików jednocześnie.
 - podpisywanie dokumentów w formacie plików XML, plików tekstowych, dokumentów PDF, plików pakietu biurowego MS Office/Open Office, archiwów ZIP, plików binarnych.
 - zgodne z eIDAS, w tym obsługujące algorytm funkcji skrótu SHA2.
 - c) oprogramowanie pozwalające na weryfikację podpisów elektronicznych kompatybilne z systemami operacyjnymi komputera, co najmniej: MS Windows: 10, 11 oraz Linux i Mac OS.

- d) oprogramowanie pozwalające na składanie podpisów kompatybilne z systemami operacyjnymi komputera, co najmniej: MS Windows 10, 11 oraz Linux i Mac OS.
- 5) Oprogramowanie do zarządzania certyfikatami na karcie kryptograficznej, w tym umożliwiające zmianę kodów PIN i PUK, rejestrację certyfikatu w systemie MS Windows, odczytanie informacji o certyfikatach na karcie, oraz przeprowadzenie odnowienia podpisu, kompatybilne, co najmniej z systemami operacyjnymi komputera MS Windows: 10 oraz 11.
- 6) Wykonawca będzie odpowiedzialny za zapewnienie niezawodnej pracy zestawów do składania kwalifikowanego podpisu elektronicznego wraz z dostarczonym oprogramowaniem.
- 7) Instrukcje obsługi dla użytkowników podpisów elektronicznych nieposiadających wiedzy technicznej, w języku polskim, a w tym co najmniej instrukcja weryfikacji ważności podpisów oraz odczytu treści dokumentu, instrukcja składania podpisów wraz z przypadkiem wielopodpisu, kontrasygnaty, znacznika czasu. Instrukcja odnowienia certyfikatu podpisu kwalifikowanego, instrukcja zarządzania certyfikatami na karcie kryptograficznej w tym wgrywanie certyfikatu, zmiana PIN, zmiana PUK, instrukcje używania i konfigurowania dostarczonego oprogramowania. Instrukcje będą udostępnione w postaci plików PDF dostarczonych wraz z zestawami do podpisu lub udostępnionych na ogólnodostępnej stronie internetowej centrum certyfikacji.

E. Wydanie certyfikatów niekwalifikowanych Certum S/MIME Sponsor ID, lub równoważnych

- 1) Wykonawca wystawi certyfikaty niekwalifikowane w sposób niepowodujący konieczności osobistego stawiennictwa subskrybenta w punkcie weryfikacji tożsamości.
- 2) Certyfikaty będą wydawane na okres 1 rok.
- 3) Wystawione certyfikaty pozwolą na zaawansowane elektroniczne podpisywanie e-mail, dokumentów PDF np. w formacie PAdES w tym dokumentów przeznaczonych do publikacji np. Elektronicznych Dzienników Urzędowych.
- 4) Dane zawarte w certyfikacie: adres e-mail, imię i nazwisko, dane Zamawiającego.
- 5) Certyfikat pozwoli na wiarygodną identyfikację posiadacza certyfikatu w sieci Internet.
- 6) Certyfikat ma posiadać gwarancję finansową min. 60 000 EU.
- 7) Zgodność z WebTrust ^{SM/™} .

2. Dodatkowe zobowiązania

- A. Wykonawca będzie świadczył usługi zaufania niezbędne dla obsługi wystawionych certyfikatów kwalifikowanych pozwalających na składanie kwalifikowanego podpisu elektronicznego zgodnie z przyjętymi procedurami i Polityką Certyfikacji, a w szczególności:
 - 1) na pisemny wniosek Zamawiającego Wykonawca zawiesi lub unieważni wskazane certyfikaty kwalifikowane.
 - 2) opublikuje unieważnione certyfikaty na liście certyfikatów odwołanych.
 - 3) udostępni możliwość pobierania z repozytorium certyfikatów.

- B. Wykonawca zobowiązuje się do informowania Zamawiającego, z odpowiednim wyprzedzeniem, o istotnych zmianach oprogramowania lub zmianach adresacji serwerów niezbędnych do świadczenia usług zaufania, weryfikacji podpisów elektronicznych, wydawania certyfikatów, lub znakowania czasem w celu zapewnienia nieprzerwanego dostępu do potrzebnych usług.
- C. Wykonawca będzie aktualizował niezbędne oprogramowanie w celu niezwłocznego dostosowania go do zmieniających się standardów, przepisów prawa, nowych wersji systemów operacyjnych komputera, JAVA, przeglądarek internetowych, nowych algorytmów, nowych długości kluczy kryptograficznych i zabezpieczenia przed wykrytymi potencjalnymi zagrożeniami bezpieczeństwa oraz błędami.
- D. Wykonawca udostępni system informatyczny (np. serwis online) pozwalający na składanie wniosków o certyfikaty niekwalifikowane Certum S/MIME Sponsor ID dla pracowników Zamawiającego przez upoważnionego pracownika Zamawiającego.
- E. Wykonawca udostępni Zamawiającemu system informatyczny (np. serwis online), będący repozytorium wydanych certyfikatów niekwalifikowanych Certum S/MIME Sponsor i pozwalający wskazanym pracownikom Zamawiającego na samodzielne zarządzanie certyfikatami niekwalifikowanymi Certum S/MIME Sponsor w zakresie co najmniej:
 - 1) Zapisywanie danych organizacji oraz szablonu zamówień
 - 2) Wysyłanie zamówień
 - 3) Wysyłanie weryfikacji
 - 4) Pobieranie certyfikatów
 - 5) Anulowanie i usuwanie odrzuconych zamówień
 - 6) Zapisywanie i usuwanie certyfikatów z archiwum
 - 7) Wyszukiwanie certyfikatów
 - 8) Unieważnianie certyfikatów
 - 9) Wystawienie duplikatu certyfikatów (Reissue).

3. Wsparcie techniczne

- 1) Wykonawca będzie świadczył usługi wsparcia merytorycznego w zakresie obsługi kwalifikowanego podpisu elektronicznego w godzinach 8.00 – 16.00 w dni robocze.
- 2) Wykonawca udostępni wszystkim użytkownikom, dla których wystawiono certyfikat kwalifikowany, w ramach powyższego zamówienia, następujące środki komunikacji: infolinię telefoniczną płatną w/g taryfy za połączenia lokalne i międzymiastowe, adres poczty elektronicznej w celu zapewnienia pomocy w przypadku problemów z obsługą podpisów elektronicznych, certyfikatów kwalifikowanych, elementów zestawów do składania podpisu elektronicznego oraz realizacji usług zaufania.
- 3) Wykonawca zapewni dostarczenie aktualizacji oprogramowania do obsługi podpisu elektronicznego w przypadku konieczności dostosowania go do zmieniających się przepisów prawa lub zmiany standardów technicznych, dostosowania do nowych wydań systemów operacyjnych komputera, usunięcia usterek, udostępnienia nowych wersji, zmian długości kluczy oraz algorytmów. Nowa wersja może być udostępniona za pośrednictwem witryny internetowej Centrum Certyfikacji.

- 4) Za konsultacje dokonane ustaloną drogą komunikacji Wykonawcy nie przysługuje dodatkowe wynagrodzenie.

4. Gwarancja

- 1) Wykonawca gwarantuje dostarczenie fabrycznie nowych elementów wchodzących w skład zestawu do składania kwalifikowanego podpisu elektronicznego.
- 2) Wykonawca zobowiązuje się dostarczać fabrycznie nowe karty kryptograficzne w przypadku, gdy do przeprowadzenia odnowienia certyfikatu kwalifikowanego konieczna będzie wymiana karty.
- 3) Wykonawca udziela 24-miesięcznej gwarancji na elementy wchodzące w skład zestawu do składania kwalifikowanego podpisu elektronicznego.
- 4) Wykonawca gwarantuje, że dostarczone lub udostępnione oprogramowanie, oraz sterowniki są wolne od złośliwego oprogramowania, nie będą zawierały reklam, oraz ukrytych funkcji szpiegujących i są bezpieczne do używania zgodnego z ich przeznaczeniem.
- 5) Wszelkie koszty związane z usuwaniem usterek objętych gwarancją ponosi Wykonawca.

5. Zgodność z przepisami prawa oraz certyfikacja

- 1) Wykonawca zapewnia zgodność z **Ustawą** wraz z aktami wykonawczymi i **eIDAS**
- 2) Wykonawca zapewnia zgodność z **WebTrust**^{SM/™} w zakresie certyfikatów niekwalifikowanych (certyfikaty S/MIME).
- 3) Wykonawca posiada **certyfikat ISO IEC 27001** lub równoważny.