Załącznik nr 2 do postępowania KA-CZL-DZP.261.2.116.2023

OPIS PRZEDMIOTU ZAMÓWIENIA

1. **Krótki opis przedmiotu zamówienia**

Przedmiotem zamówienia jest świadczenie usług zaufania – tworzenia i wydawania kwalifikowanych certyfikatów podpisu elektronicznego wraz ze świadczeniem usług komplementarnych dla wskazanych pracowników Uniwersytetu Ekonomicznego we Wrocławiu w związku z realizacją projektu „Nowa jakość – nowe możliwości. Zintegrowany program rozwoju uczelni"

Wymagania zamawiającego	Opis
Liczba podpisów:	100
Planowany termin realizacji usługi	Do 18.12.2023
Opis przedmiotu zamówienia	1. 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, dla których wydawane są certyfikaty, w tym: zapewnienie nieodpłatnego dostępu do autoryzowanego punktu weryfikacji tożsamości zlokalizowanego na terenie Wrocławia i Jeleniej Góry lub świadczenie usługi grupowej weryfikacji tożsamości w siedzibie Zamawiającego; 3) 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; 2. Zamawiający wraz ze Zleceniem przekaże Wykonawcy niezbędne dane do przeprowadzenia procesu wystawienia certyfikatu kwalifikowanego zgodnie z procedurami i Polityką Certyfikacji Wykonawcy. 3. Od momentu otrzymania zlecenia Wykonawca w terminie nie dłuższym niż dwóch dni roboczych skontaktuje się z Zamawiającym w celu ustalenia terminu i sposobu weryfikacji tożsamości wskazanych osób. 4. Wykonawca nie będzie pobierał od Zamawiającego żadnych dodatkowych opłat za przeprowadzenie weryfikacji tożsamości. 5. Wykonawca wystawi certyfikat ważny przez okres 2 lat. 6. Certyfikat powinien spełniać wymagania stawiane w Ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej

	(Ustawa) oraz w Rozporządzeniu 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). 7. Spełniać wymagania aktów wykonawczych do Ustawy.

1. **Warunki realizacji usługi**

Certyfikat kwalifikowany do składania kwalifikowanego podpisu elektronicznego powinien:

1) Posiadać okres ważności 2 lata,

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 (System Elektronicznego Zarządzania Dokumentami)

1. **Zestaw do składania certyfikowanego podpisu elektronicznego powinien zawierać:** Certyfikat kwalifikowany do składania kwalifikowanego podpisu elektronicznego zgodny z wymaganiami wskazanymi w **Ustawie** o okresie ważności 2 lat.
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, tzw. token (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:, 7, 8, 10, 11 Dostępne sterowniki dla systemów z rodziny Linux, Mac OS oraz Android.

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:
   b. weryfikację podpisu elektronicznego złożonego przy użyciu certyfikatu kwalifikowanego wystawionego przez jedno z dostępnych w Polsce kwalifikowanych Centrów Certyfikacji.
   c. Zgodne z eIDAS, w tym obsługujące algorytm funkcji skrótu SHA2 oraz różne długości kluczy kryptograficznych.
5. Oprogramowanie do składania podpisu elektronicznego powinno co najmniej umożliwiać realizację następujących funkcjonalności:
   a. złożenie podpisu elektronicznego,
   b. złożenie kontrasygnaty dla podpisanego dokumentu podpisem elektronicznym,
   c. obsługę wielopodpisu,
   d. znakowania czasem.
   e. składanie podpisów elektronicznych wewnętrznych, oraz zewnętrznych w formacie XAdES i podpisów wewnętrznych w formacie PAdES.
   f. składanie podpisu elektronicznego wraz z rodzajem zobowiązania „Proof of approval", oraz bez zobowiązania.
   g. podpisywanie zarówno pojedynczych plików jak też wielu plików jednocześnie.
   h. podpisywanie dokumentów w formacie plików XML, plików tekstowych, dokumentów PDF, plików pakietu biurowego MS Office/Open Office, archiwów ZIP, plików binarnych.
   i. zgodne z eIDAS, w tym obsługujące algorytm funkcji skrótu SHA2.
6. Oprogramowanie pozwalające na weryfikację podpisów elektronicznych kompatybilne z systemami operacyjnymi komputera, co najmniej: MS Windows: 7, 8, 10, 11 oraz Linux i Mac OS. Oprogramowanie powinno umożliwić weryfikację wszelkich podpisów elektronicznych w tym składanych za pomocą certyfikatów kwalifikowanych wystawionych przez centra certyfikacji zarejestrowane w Polsce.

Oprogramowanie służące do weryfikacji podpisów elektronicznych powinno być bezpłatnie udostępnione do pobrania na witrynie internetowej Centrum Certyfikacji, lub w odpowiednim dla danego systemu operacyjnego komputera/urządzenia mobilnego sklepie. Oprogramowanie powinno być zgodne z aktualnie obowiązującymi przepisami w tym eIDAS.

7. Oprogramowanie pozwalające na składanie podpisów kompatybilne z systemami operacyjnymi komputera, co najmniej: MS Windows 7, 8,10,11.
8. Oprogramowanie do zarządzana 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, 7, 8, 10,11
9. Wykonawca będzie odpowiedzialny za zapewnienie niezawodnej pracy zestawów do składania kwalifikowanego podpisu elektronicznego wraz z dostarczonym oprogramowaniem.
10. 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. 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.

1. 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.

Wsparcie techniczne

1) Wykonawca będzie świadczył usługi wsparcia merytorycznego oraz technicznego 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.

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.