1. Konfiguracja stanowiska pod podpis

*W przypadku korzystania z podpisu zaufanego można pominąć konfigurację stanowiska i przejść od razu do sprawdzenia podpisanego dokumentu.

**W celu użycia mobilnego podpisu MSzafir w aplikacji Szafir SDK należy dodać wirtualną kartę MSzafir w oprogramowaniu CloudSinger zgodnie z instrukcją dostępną pod poniższym linkiem:

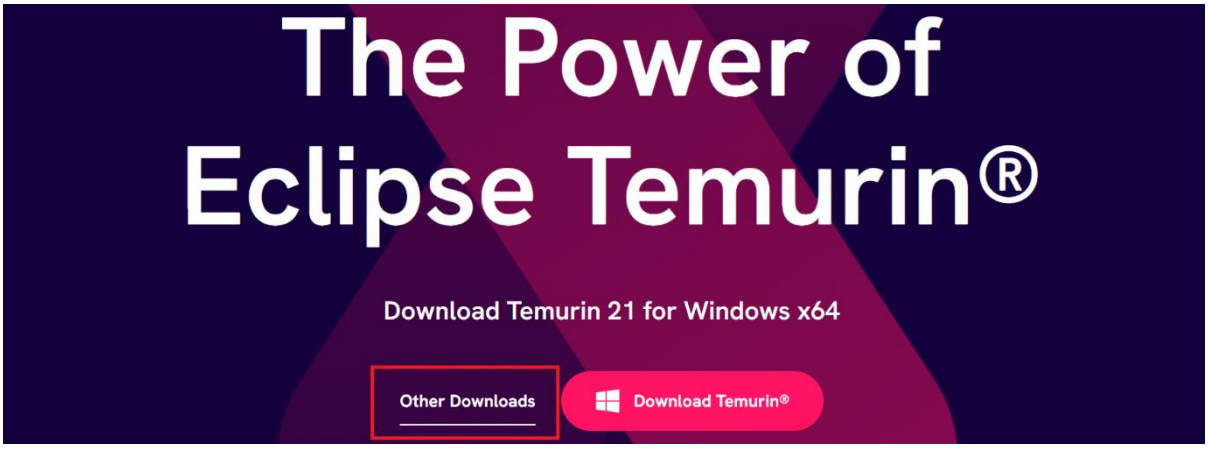
https://www.elektronicznypodpis.pl/storage/file/core_files/2024/7/3/3ae2a9ac5c3eb539e493d8b7373f05df/jak_wykorzystac_certyfikat_mszafir_w_dowolnej_aplikacji_podpisujacej_windows.pdf

Pierwszym krokiem konfiguracji będzie zainstalowanie oprogramowania Java w wersji OpenJDK wydawanej na licencji EPL (Eclipse Public License - v 2.0). Rekomendowaną wersją jest Temurin 17LTS lub wyższa. Istotne, aby to były wersje LTS (long-term suport).

Można je pobrać za darmo ze strony:

https://adoptium.net/

Po wejściu na wskazaną stronę należy wybrać przycisk „other downloads”.



RYSUNEK 1: PRZYCISK „OTHER DOWNLOADS” NA STRONIE HTTPS://ADOPTIUM.NET/

Następnie w poziomym menu [1] należy wybrać odpowiednią wersję oprogramowania JDK 17 LTS [1], a następnie użyć ikony pobierania [2 lub 3] przy systemie operacyjnym, który jest zainstalowany na konfigurowanym stanowisku komputerowym.

RYSUNEK 2: WYBÓR WERSJI OPROGRAMOWANIA JAVA NA STRONIE HTTPS://ADOPTIUM.NET/

Bezpośredni link do oprogramowania dla Windows:

https://adoptium.net/temurin/releases/?os=windows&arch=x64&package=jdk&version=17

Bezpośredni link do oprogramowania dla Mac:

https://adoptium.net/temurin/releases/?os=mac&arch=x64&package=jdk&version=17

***Przeglądarka Opera nie wspiera dodatku Szafir SDK i uniemożliwia złożenie podpisu.**

Następnie należy upewnić się, że na stacji roboczej jest zainstalowane aktualne oprogramowanie dołączone do certyfikatu jak również, że podpis jest zaimportowany do przeglądarki. Poniżej ścieżki dostępu dla najpopularniejszych przeglądarek:

Microsoft Edge – ustawienia ->prywatność, wyszukiwanie i usługi -> zabezpieczenia -> zarządzaj certyfikatami

Google Chrome – ustawienia -> prywatność i bezpieczeństwo -> bezpieczeństwo -> zarządzaj certyfikatami

Firefox – opcje -> prywatność i bezpieczeństwo -> wyświetl certyfikaty

Prawidłowo zaimportowany certyfikat powinien się wyświetlić w zakładce:

„osobisty” na przeglądarkach Microsoft Edge i Google Chrome

„użytkownik” na przeglądarce Firefox.

Gdyby certyfikat nie był widoczny, należy skontaktować się z wystawcą certyfikatu i poprosić o pomoc przy zaimportowaniu certyfikatu do przeglądarki.

Import podpisu do przeglądarki nie dotyczy komputerów typu Mac.

Na komputerach typu Mac może być konieczne zainstalowanie dodatkowego oprogramowania:

Dodatkowe oprogramowanie dla Mac

Po wykonaniu powyższych czynności należy wejść na stronę:

https://oneplace.marketplanet.pl/sprawdz-podpis

Po wejściu na stronę pojawi się możliwość wyboru rodzaju sprawdzanego podpisu.

A) Podpis kwalifikowany elektroniczny [1]
B) Polski E-dowód [2]
C) Dokument podpisany za pomocą Podpisu Zaufanego EPUAP [3]

RYSUNEK 3: WYBÓR RODZAJU PODPISU ELEKTRONICZNEGO

A) PODPIS KWALIFIKOWANY ELEKTRONICZNY

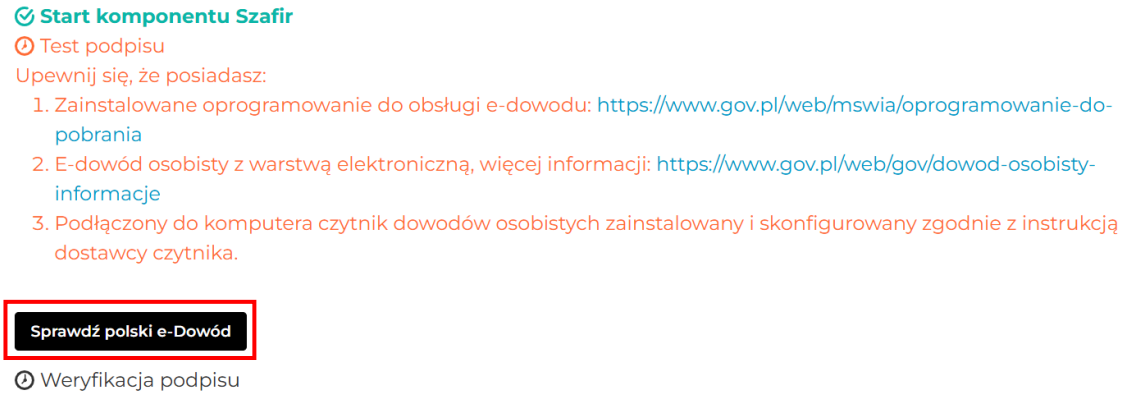
Użycie przycisku “sprawdź podpis” spowoduje uruchomienie komponentu Szafir.

RYSUNEK 4: TEST PODPISU - PODPIS KWALIFIKOWANY

Uwaga! Prosimy, aby w aukcji elektronicznej (gdzie Zamawiający wymaga potwierdzenia złożenia oferty za pomocą podpisu kwalifikowanego), w momencie pracy na przeglądarce w trybie prywatnym (incognito), podczas konfiguracji kontrolki Szafir Host zaznaczać opcje dodania dodatku do przeglądarek Szafir SDK Web również do wskazanych przeglądarek prywatnych. Brak zaznaczenia rozszerzenia dodatku na przeglądarki prywatne spowoduje, że konsola aukcyjna przy każdym postąpieniu będzie wymuszała aktualizację kontrolki Szafir Host. Może to wydłużyć czas, aby prawidłowo zaakceptować postąpienia w aukcji elektronicznej.

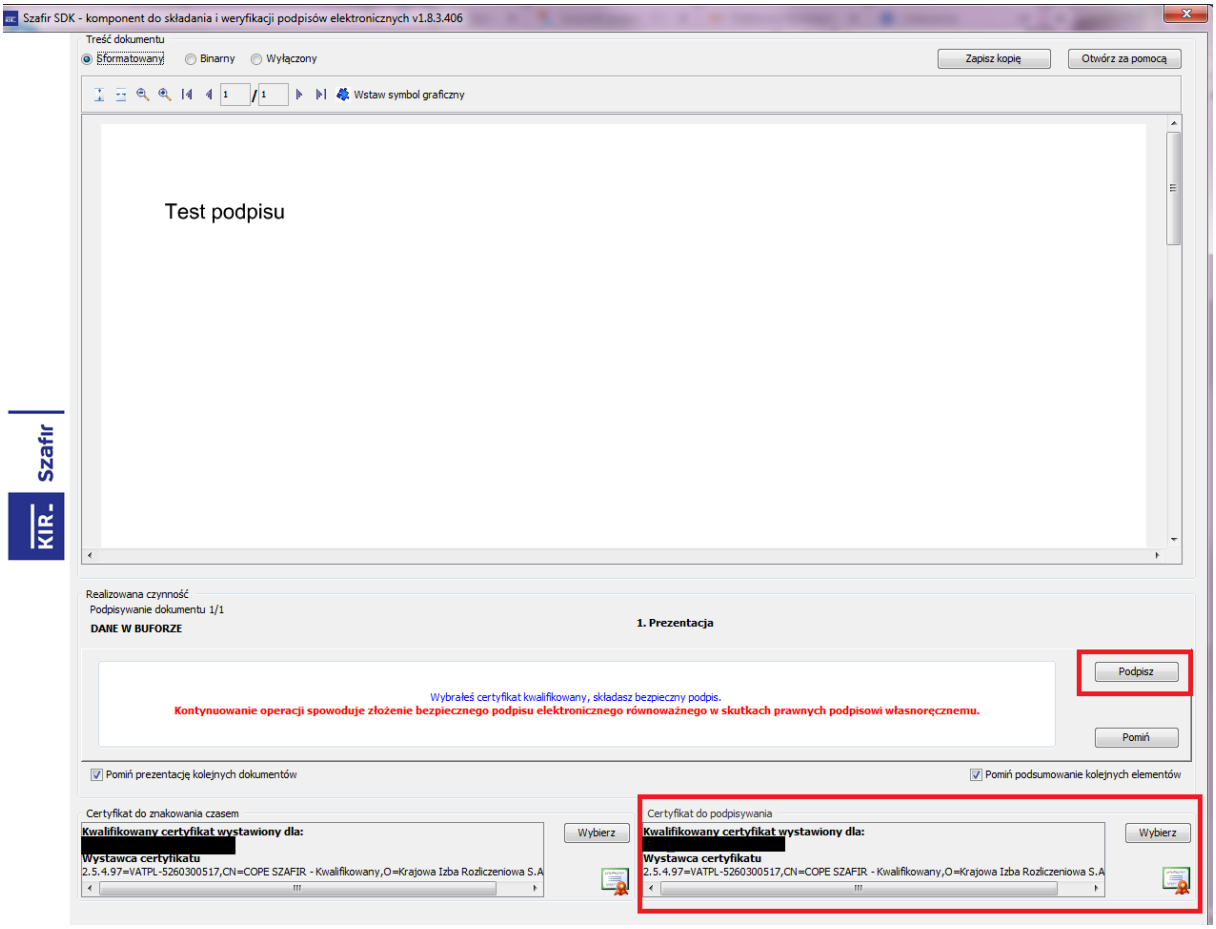
B) POLSKI E-DOWÓD

Użycie przycisku “sprawdź polski e-dowód” spowoduje uruchomienie komponentu Szafir.



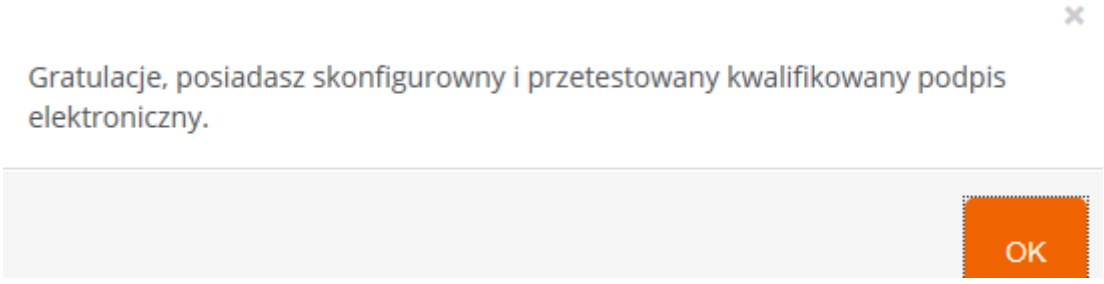
RYSUNEK 5: TEST PODPISU - E-DOWÓD

TEST PODPISU NALEŻY SFINALIZOWAĆ POPRZEZ WYBRANIE CERTYFIKATU DO PODPISU/POLSKIEGO E-DOWODU I PODPISANIE PLIKU TESTOWEGO.



RYSUNEK 6: APLIKACJA SZAFIR SDK

Po zaakceptowaniu krótkiego podsumowania pojawi się następujący komunikat

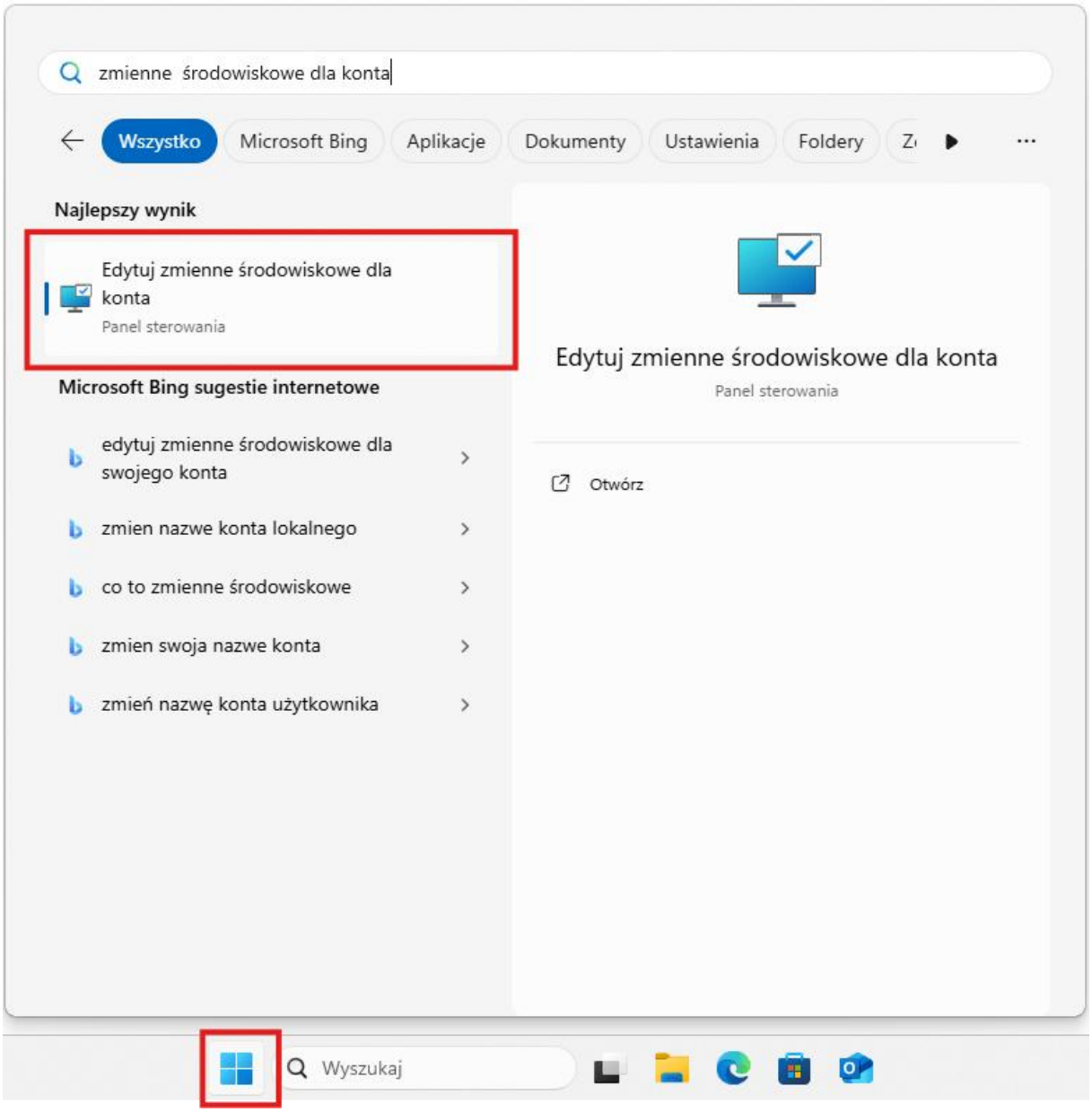


RYSUNEK 7: KOMUNIKAT PO PRAWIDŁOWYM SKONFIGUROWANIU STANOWISKA

UWAGA! Dla użytkowników systemu Operacyjnego Windows

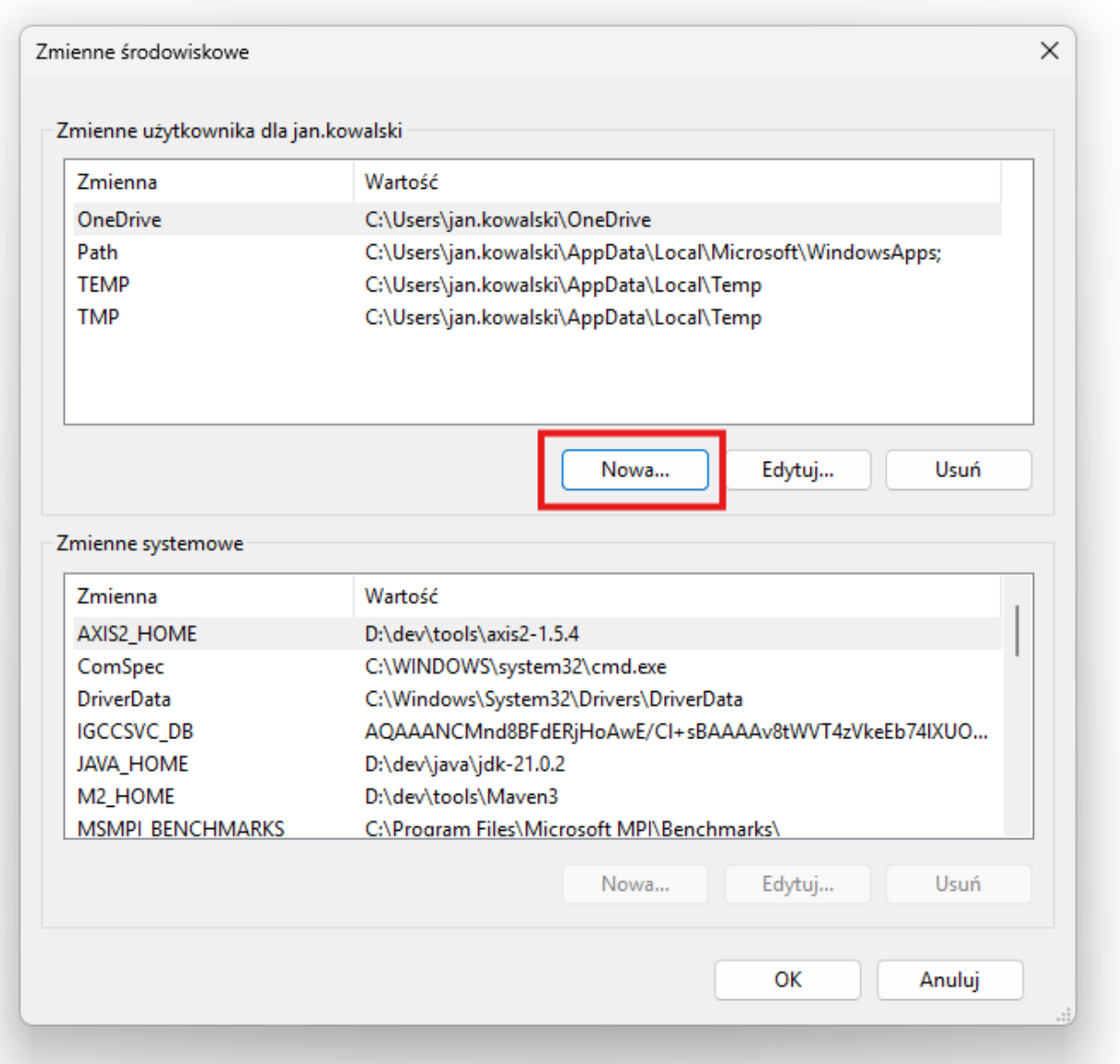
Obecna wersja kontrolki, po aktualizacji w grudniu 2025 roku do poprawnego działania wymaga dodania zmiennej środowiskowej do systemu Windows o nazwie PKCS11_USE_240_ONLY i wartości true.

W celu dodania zmiennej środowiskowej należy uruchomić menu „Start" i wyszukać frazę „Zmienne środowiskowe dla konta" i wybrać pozycję „**Edytuj zmienne środowiskowe dla konta**" (UWAGA! Nie pomylić z podobną opcją „Edytuj zmienne środowiskowe dla systemu").



RYSUNEK 8: EDYCJA ZMIENNEJ ŚRODOWISKOWEJ

Następnie w oknie wybrać przycisk „Nowa” w sekcji „Zmienne użytkownika dla XXX”, gdzie XXX jest nazwą zalogowanego do systemu użytkownika.



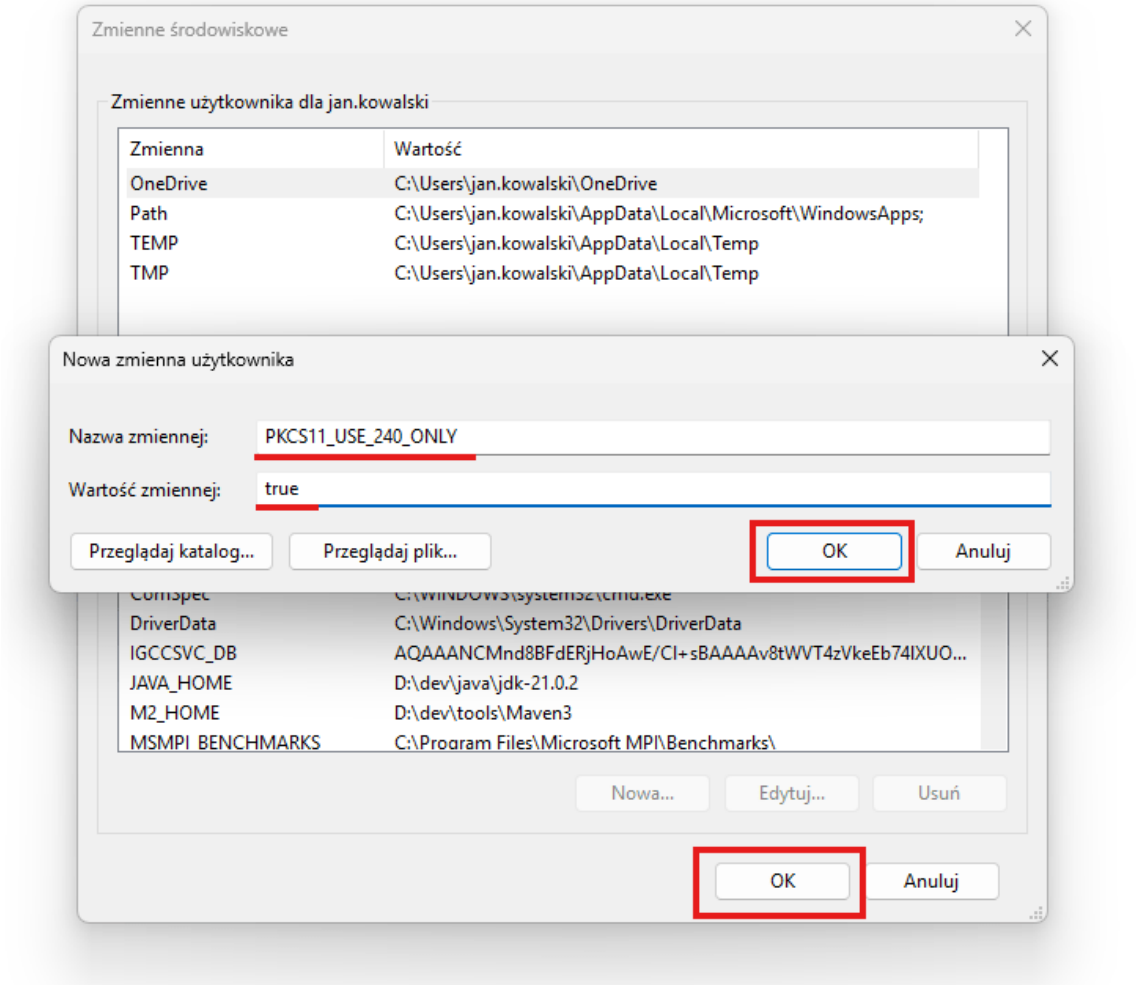
RYSUNEK 9: NOWA ZMIENNA ŚRODOWISKOWA

Kolejnym krokiem jest uzupełnienie formularza w oknie „Nowa zmienna użytkownika”:

Nazwa zmiennej: PKCS11_USE_240_ONLY

Wartość zmiennej: true

Oraz dwukrotne zatwierdzenie zmian przyciskami „OK”.

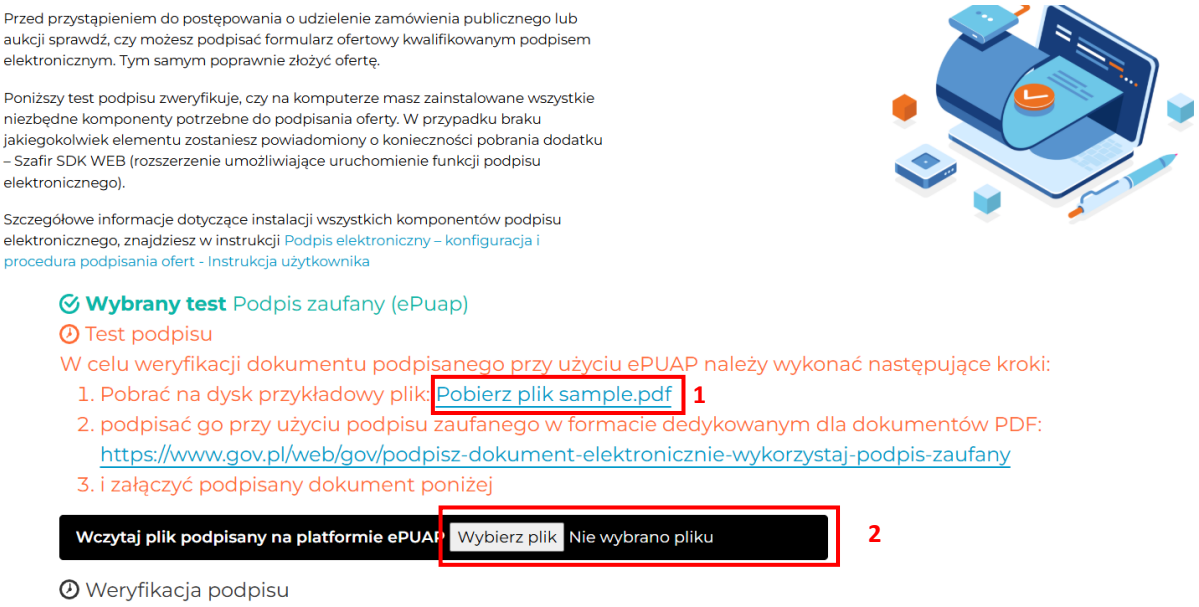


RYSUNEK 10: WPROWADZENIE DANYCH NOWEJ ZMIENNEJ ŚRODOWISKOWEJ

WAŻNE! Po dokonaniu zmian należy uruchomić ponownie komputer, aby zmiany były widoczne i dostępne dla przeglądarki internetowej.

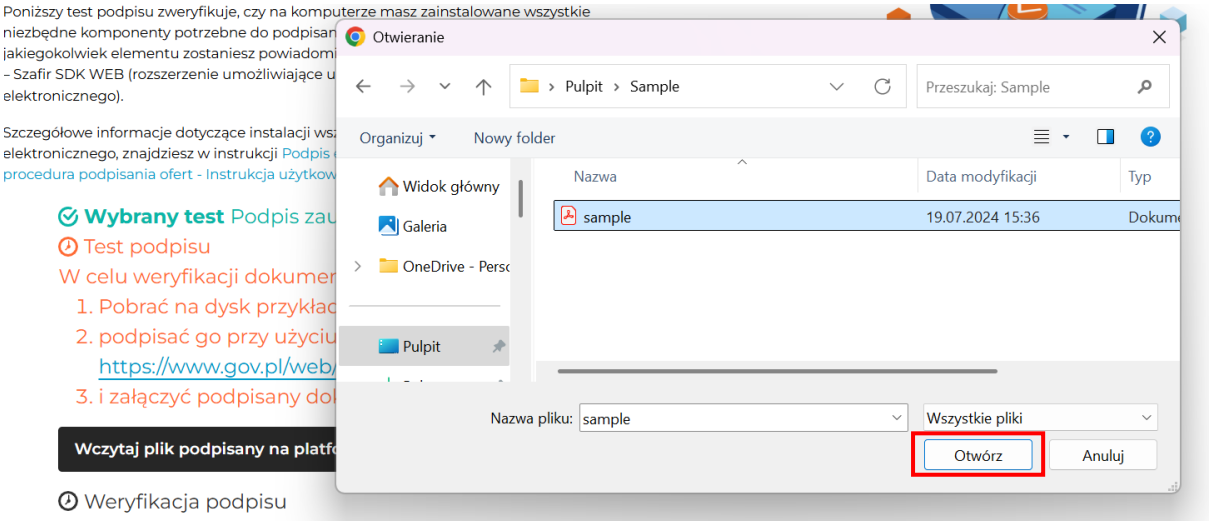
C) DOKUMENT PODPISANY ZA POMOCĄ PODPISU ZAUFANEGO (EPUAP)

Zgodnie z wyświetlaną instrukcją należy pobrać testowy dokument [1] podpisać go za pomocą Podpisu Zaufanego oraz dołączyć za pomocą przycisku „wybierz” [2].



RYSUNEK 11: TEST PODPISU - EPUAP

Pojawi się okno w którym należy wybrać podpisany plik z komputera i dodać go za pomocą przycisku „Otwórz”.



Rysunek 12: Test podpisu - EPUAP, wybór podpisanego pliku z komputera