



Moduł weryfikacji podpisu EZD PUW

Wersja 3.100.1 BETA

Data publikacji: 16.12.2020



Spis treści

1	Konfiguracja modułu weryfikacji podpisu	3
1.1	Konfiguracja modułu zewnętrznego weryfikacji podpisu (JAVA)	3
1.2	Ustawienia	4
2	Funkcjonalności modułu weryfikacji podpisu.....	4
2.1	Dodawanie dokumentu	4
2.2	Informacja o złożonych podpisach	6

1 Konfiguracja modułu weryfikacji podpisu

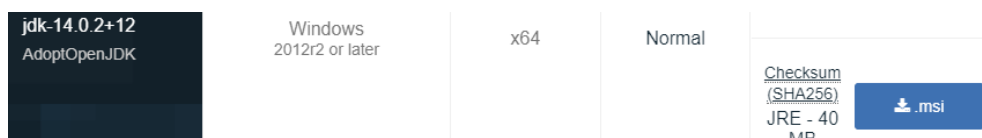
1.1 Konfiguracja modułu zewnętrznego weryfikacji podpisu (JAVA)

Moduł Weryfikacji Podpisu Elektronicznego (WPE) dystrybuowany jest w postaci pliku wykonywalnego **nask-hsign.jar**

Uruchomieniu modułu weryfikacji podpisu wymaga zainstalowania na serwerze aplikacyjnym EZD PUW środowiska uruchomieniowego JRE. Konfiguracja opisana w tej instrukcji opiera się na środowisku udostępnionym przez AdoptOpenJDK.

Pakiet msi jest dostępny do pobrania z strony:

<https://adoptopenjdk.net/releases.html?variant=openjdk14&jvmVariant=hotspot>



Po instalacji pakietu na serwerze oraz wywołaniu w oknie „cmd” komendy `java -version` powinniśmy otrzymać informacji o zainstalowanym JRE.

```
C:\Windows\System32\cmd.exe

C:\>java -version
openjdk version "14.0.2" 2020-07-14
OpenJDK Runtime Environment AdoptOpenJDK (build 14.0.2+12)
OpenJDK 64-Bit Server VM AdoptOpenJDK (build 14.0.2+12, mixed mode, sharing)

C:\>_
```

W przypadku błędu należy upewnić się, że instalator dodał ścieżkę do katalogu zawierającego binaria instalowanego środowiska do parametru systemowego PATH:

```
C:\Windows\System32\cmd.exe

C:\>path
PATH=C:\Program Files\AdoptOpenJDK\jre-14.0.2.12-hotspot\bin;C:\WindowsPowerShell\v1.0\;C:\Program Files\Microsoft\Web Platform Ins

C:\>_
```

Moduł weryfikacji podpisu należy uruchomić komendą:

`java -jar nask.hsign.jar --server.port=9090`





Przykładowy plik wsadowym **nask.hsign.bat** dostępny jest na **ezd.gov.pl**. Pobrany plik wsadowy należy uruchamiać z katalogu, do którego został przekopiowany plik **nask.hsign.jar**

Parametr **--server.port=9090** spowoduje, że usługa zostanie uruchomiona na porcie 9090

Numer podanego portu musi być zgodny z ustawieniami przedstawionymi w punkcie 1.2 instrukcji z parametrem: **Weryfikacja podpisu url modułu zewnętrznego**

1.2 Ustawienia

W zakładce Ustawienia znajdującej się w sekcji Administracja należy skonfigurować ustawienia znajdujące się w grupie weryfikacja podpisu przez moduł zewnętrzny

Weryfikacja podpisu przez moduł zewnętrzny		
Weryfikacja podpisu - włączona <small>zewnetrznaWeryfikacjaPodpisu.enable</small>	<input checked="" type="checkbox"/> TAK	
Weryfikacja podpisu - cron <small>zewnetrznaWeryfikacjaPodpisu.cron</small>	<input type="text" value="0 0/1 * 1/1 * ? *"/>	
Weryfikacja podpisu url modułu zewnętrznego <small>zewnetrznaWeryfikacjaPodpisu.url</small>	<input type="text" value="http://adres:port/"/>	
Weryfikacja podpisu ilość prób pobrania weryfikacji <small>zewnetrznaWeryfikacjaPodpisu.iloscProb</small>	<input type="text" value="20"/>	
Weryfikacja podpisu czas odstępu między próbami (w milisekundach) <small>zewnetrznaWeryfikacjaPodpisu.odstepMiedzyProbami</small>	<input type="text" value="500"/>	

Do prawidłowego działania modułu weryfikacji podpisu należy skonfigurować następujące ustawienia:

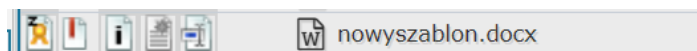
- `zewnetrznaWeryfikacjaPodpisu.enable` – włączenie modułu weryfikacji podpisu
- `zewnetrznaWeryfikacjaPodpisu.cron` – czas wywołania tasku weryfikacji podpisu w WinService (czyli faktyczne wywołanie API zewnętrznego modułu weryfikacji podpisu), domyślnie należy wprowadzić
- `0 0/1 * 1/1 * ? *`, oznacza odświeżenie co minutę
- `zewnetrznaWeryfikacjaPodpisu.url` – adres fizyczny serwera, na którym wystawiony jest moduł weryfikacji podpisu
- `zewnetrznaWeryfikacjaPodpisu.iloscProb` – ilość prób pobrania weryfikacji (gdy się nie poda domyślnie jest 5)
- `zewnetrznaWeryfikacjaPodpisu.odstepMiedzyProbami` – czas odstępu między próbami (w milisekundach) (gdy się nie poda domyślnie jest 100)

2 Funkcjonalności modułu weryfikacji podpisu

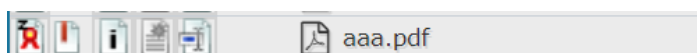
2.1 Dodawanie dokumentu

Weryfikator zwraca 4 statusy:

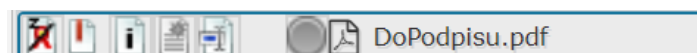
- Oczekiwanie na wynik weryfikacji



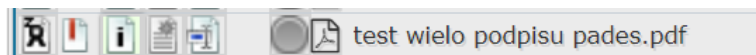
- poprawnie zweryfikowany



- niepoprawnie zweryfikowany



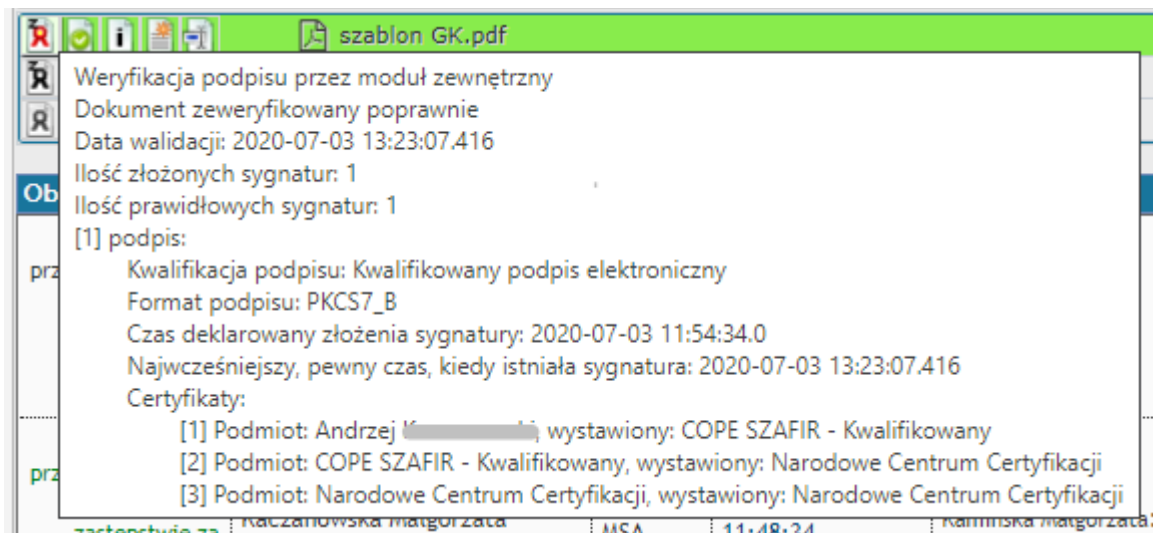
- błąd zewnętrznego modułu weryfikacji



Wynik weryfikacji można zobaczyć po najechnaniu na ikonę



lub



Dodatkowo szczegółowy wynik znajduje się w oknie po kliknięciu na



Weryfikacja dokumentu: dokument test weryfikacji podpisu.pdf

Złożone podpisy / akceptacje:

	Podpisujący	Data podpisu	Uwagi
1		2020-07-15 12:01:15	

Odśwież

Weryfikacja podpisu EZD (id dokumentu: 2880235)

Podpis zweryfikowany PRAWIDŁOWO
Data walidacji: 2020-07-15 12:02:03
Ilość złożonych sygnatur: 1
Ilość prawidłowych sygnatur: 1

	Podpisujący (ścieżka certyfikacyjna)
	Uwagi
1	<div> , wystawiony: COPE SZAFIR - Kwalifikowany COPE SZAFIR - Kwalifikowany, wystawiony: Narodowe Centrum Certyfikacji Narodowe Centrum Certyfikacji, wystawiony: Narodowe Centrum Certyfikacji </div> <div> Kwalifikacja podpisu: Kwalifikowany podpis elektroniczny Format podpisu: PKCS7_B Czas deklarowany złożenia sygnatury: 2020-07-15 12:01:15 Najwcześniejszy, pewny czas, kiedy istniała sygnatura: 2020-07-15 12:02:03 </div>

2.2 Informacja o złożonych podpisach

W menu podręcznym zweryfikowanego dokumentu pdf dostępny jest wydruk „Informacja o złożonych podpisach”



Informacja o złożonych podpisach

Nazwa dokumentu	test test.pdf
Data weryfikacji	23.11.2020 16:34
Dokument zweryfikowany	PRAWIDŁOWO
Liczba złożonych podpisów	1

Sygnatura 1 z 1	
Dane podpisującego	██████████
Kwalifikacja sygnatury	Kwalifikowany podpis elektroniczny
Czas deklarowany złożenia sygnatury	23.11.2020 16:32
Czas deklarowany złożenia sygnatury	23.11.2020 16:32

Czytelny podpis sporządzającego wydruk: