

Pierwsze kroki w konfiguracji integracji Comarch BPM z usługą e-Doręczenia – generowanie żądania certyfikatu CSR i zakup pieczęci elektronicznej lub kwalifikowanego podpisu

W systemie Comarch BPM (dawniej DMS) istnieje możliwość [integracji z usługą e-Doręczenia](#).

Integracja polega na [możliwości pobierania wiadomości przychodzących na skrzynkę](#) oraz na [możliwości wysyłania wiadomości w ramach usługi e-Doręczenia z poziomu systemu Comarch BPM \(dawniej DMS\)](#).

Aby zintegrować system do zarządzania dokumentami (np. Comarch BPM) z usługą e-Doręczenia **konieczne jest posiadanie kwalifikowanego certyfikatu**. W związku z tym podmioty niepubliczne – m.in. spółki, które chcą zintegrować Comarch BPM (dawniej DMS) z usługą e-Doręczenia – w celu pobierania i wysyłania wiadomości są **zobligowane do zakupu pieczęci elektronicznej lub kwalifikowanego podpisu**.

Do integracji Comarch BPM (dawniej DMS) z usługą e-Doręczenia, rekomendowany jest [zakup Pieczęci elektronicznej Szafir](#) wystawianej przez **Krajową Izbę Rozliczeniową** z wykorzystaniem żądania CSR.

[Aby zakupić Pieczęć elektroniczną Szafir, należy:](#)

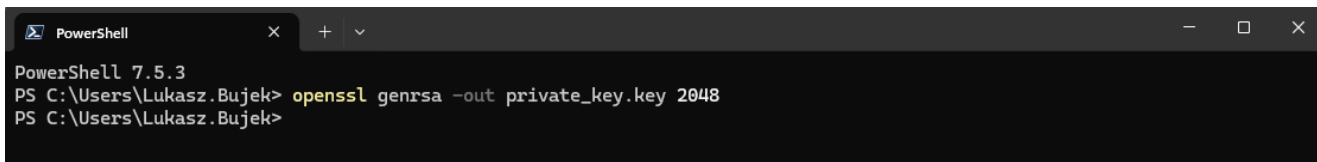
1. [Wygenerować żądanie certyfikatu CSR](#) – poprzez wykorzystanie

Środowiska OpenSSL

- OpenSSL to oprogramowanie open source, oferujące prosty interfejs wiersza polecenia służący do generowania kluczy. Oprogramowanie dostępne jest np. na stronie: <https://slproweb.com/products/Win32OpenSSL.html>
- Do przygotowania żądania CSR potrzebny będzie **klucz prywatny**:
 - Aby **wygenerować klucz prywatny**, należy przejść do terminala i użyć polecenia:

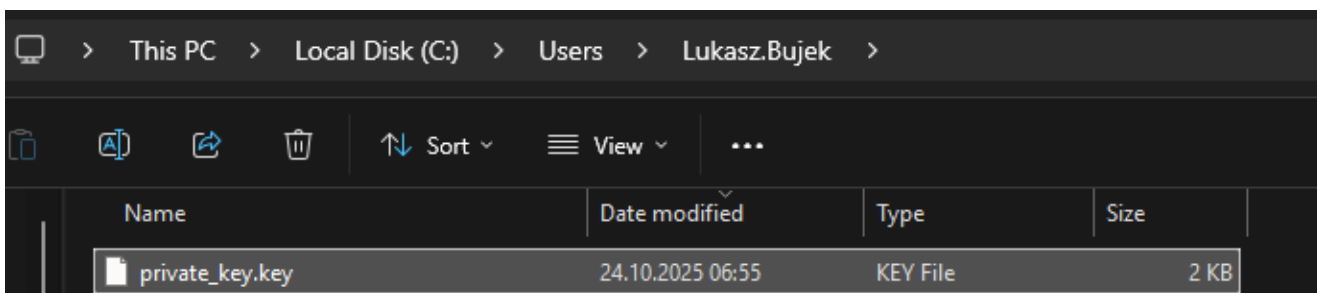
```
openssl genrsa -out private_key.key 2048
```

- Polecenie tworzy **klucz prywatny** o nazwie **private_key.key** o długości 2048



```
PowerShell 7.5.3
PS C:\Users\Lukasz.Bujek> openssl genrsa -out private_key.key 2048
PS C:\Users\Lukasz.Bujek>
```

Wprowadzanie polecenia w terminalu



Nowoutworzony klucz prywatny o nazwie private_key.key

Uwaga

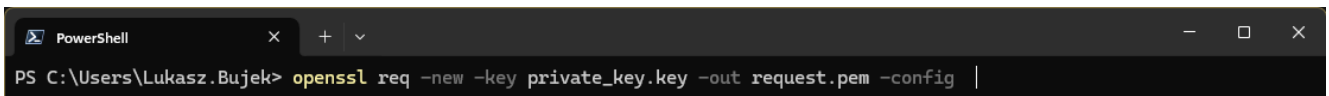
Plik `private_key.key` zostanie utworzony domyślnie w bieżącym katalogu roboczym, z którego uruchomiono polecenie.

Bezwzględnie należy zabezpieczyć klucz prywatny – nie może być udostępniany nikomu.

- Następnie **za pomocą klucza prywatnego zostanie utworzone żądanie(CSR)**: do konsoli należy wkleić i wykonać komendę:

```
openssl req -new -key private_key.key -out request.pem
```

W efekcie otrzymamy **plik request.pem z zapisanym żądaniem CSR**, wygenerowany za pomocą klucza prywatnego `private_key.key`

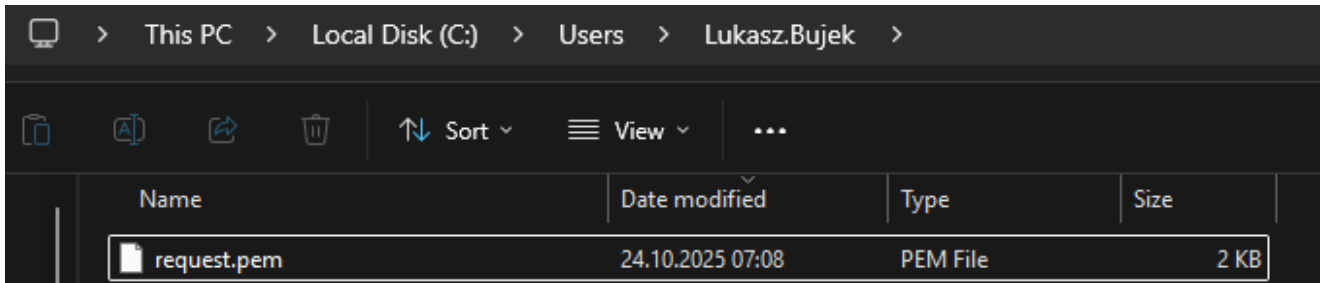


```
PowerShell
PS C:\Users\Lukasz.Bujek> openssl req -new -key private_key.key -out request.pem -config |
```

Wprowadzanie polecenia w terminalu, aby utworzyć żądanie CSR

- W trakcie wykonywania komendy, w konsoli **zostanie wyświetlony komunikat w którym trzeba będzie podać dodatkowe informacje**:
 - CountryName(kod kraju w formacie dwuliterowym),
 - State or Province Name(województwo),
 - Locality Name(miasto),
 - Organization Name(pełna nazwa organizacji),

- Organizational Unit Name(dział organizacji),
- Common Name(nazwa lub domena dla której wystawiany jest certyfikat).

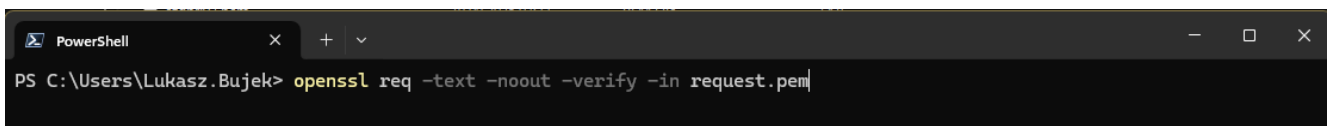


Nowoutworzone żądanie PEM

- Po utworzeniu żądania CSR można **zweryfikować** jego zawartość za pomocą polecenia:

```
openssl req -text -noout -verify -in request.pem
```

Wyświetlony wynik powinien być zgodny z podanymi danymi



Wprowadzanie w terminalu polecenia weryfikującego żądanie PEM

```
PowerShell
PS C:\Users\Lukasz.Bujek> openssl req -text -noout -verify -in request.pem -config "C:\Program Files\OpenSSL-Win64\bin\cnf\openssl.cnf"
Certificate request self-signature verify OK
Certificate Request:
Data:
  Version: 1 (0x0)
  Subject: C=PL, ST=Some-State, L=Lublin, O=Test Company, OU=BPMTest, emailAddress=lukasz.bujek@comarch.pl
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
        00:b0:66:99:50:97:1a:f4:ff:2b:4f:25:15:d7:a8:
        7a:b8:2a:cd:cd:13:3d:7c:6c:b0:1a:1e:a9:8e:6f:
        b9:77:28:71:0c:6a:3e:79:12:12:7e:93:4c:d8:a0:
        b4:08:f7:97:37:3f:e8:12:fc:ef:e3:4a:6f:b9:f8:
        2e:51:0d:64:b8:ff:da:78:92:09:10:8e:9d:1b:c7:
        e5:39:86:7d:d6:99:30:a2:87:ec:a2:93:82:00:6e:
        1e:6b:7b:33:40:60:01:e5:9f:17:ed:68:67:a4:56:
        62:72:14:53:92:c8:a1:e1:97:54:21:a4:9a:51:19:
        af:ad:a5:bb:b7:05:f0:fb:b3:4c:53:f3:69:a5:56:
        f8:40:72:6e:2d:c6:99:91:5d:f0:b2:86:a6:1e:ee:
        a6:6b:91:73:61:b9:1c:9c:3d:98:2e:e0:da:1a:4e:
        f8:18:f1:4a:b5:de:61:c0:00:2e:d1:58:0f:8b:b0:
        d7:83:fe:c9:7b:7d:de:8b:a1:6c:89:da:8f:d4:32:
        89:de:04:e7:cf:9d:46:0e:ec:b2:03:d1:8f:b4:e2:
        ce:eb:a5:f8:d4:59:01:98:dc:a4:77:83:d1:cd:29:
        2c:0a:96:34:d1:e0:89:a6:ca:f1:fb:7c:fd:df:83:
        0a:e0:a5:a3:28:e4:d4:27:af:83:1a:eb:41:33:1e:
        21:49
      Exponent: 65537 (0x10001)
  Attributes:
    (none)
  Requested Extensions:
  Signature Algorithm: sha256WithRSAEncryption
  Signature Value:
    73:a8:3b:a1:4a:f5:c8:4b:43:77:16:50:d3:b5:87:8a:cc:c5:
    dd:bc:e2:e2:39:11:d1:0c:2b:a6:f5:33:ef:0f:3d:89:88:e2:
    43:6a:70:83:35:db:e8:6e:0d:e2:f3:92:5d:bf:f7:54:1d:cc:
    85:42:99:42:05:f8:e9:88:5d:bb:04:20:29:ac:c8:fb:e4:a1:
    0a:4a:1b:25:a4:92:4d:b2:d7:9f:3c:3d:36:65:f9:02:35:f0:
    53:99:fe:d2:46:42:df:4d:49:8b:4b:cc:b7:2d:cd:a1:21:dc:
    a8:d6:c5:6c:39:c4:8d:7b:98:72:ce:c1:d3:ab:ad:76:d2:bc:
    80:e1:94:a2:fa:26:82:da:37:a1:da:ed:b4:1e:08:6e:8c:5f:
    04:f4:0b:27:75:ba:fb:5f:19:90:f2:6c:1c:9f:05:e3:79:23:
    da:78:39:45:dc:a2:be:60:41:91:37:e4:4d:87:44:4a:3e:bc:
    5b:ce:36:af:e8:9b:b9:7b:6c:4e:da:4d:18:35:88:9d:76:d4:
    20:c8:0d:6d:57:a0:26:1d:5c:ff:1e:f0:84:6e:0d:5c:96:4e:
    da:e4:d2:fe:e7:ef:b5:de:c3:a8:2e:2b:23:c0:33:36:a2:09:
    04:9c:e1:87:91:fd:db:15:69:8f:a5:58:a7:a9:90:f8:05:45:
    47:c8:ce:53
```

Wyniki wyświetlone po wprowadzeniu polecenia weryfikującego żądanie PEM

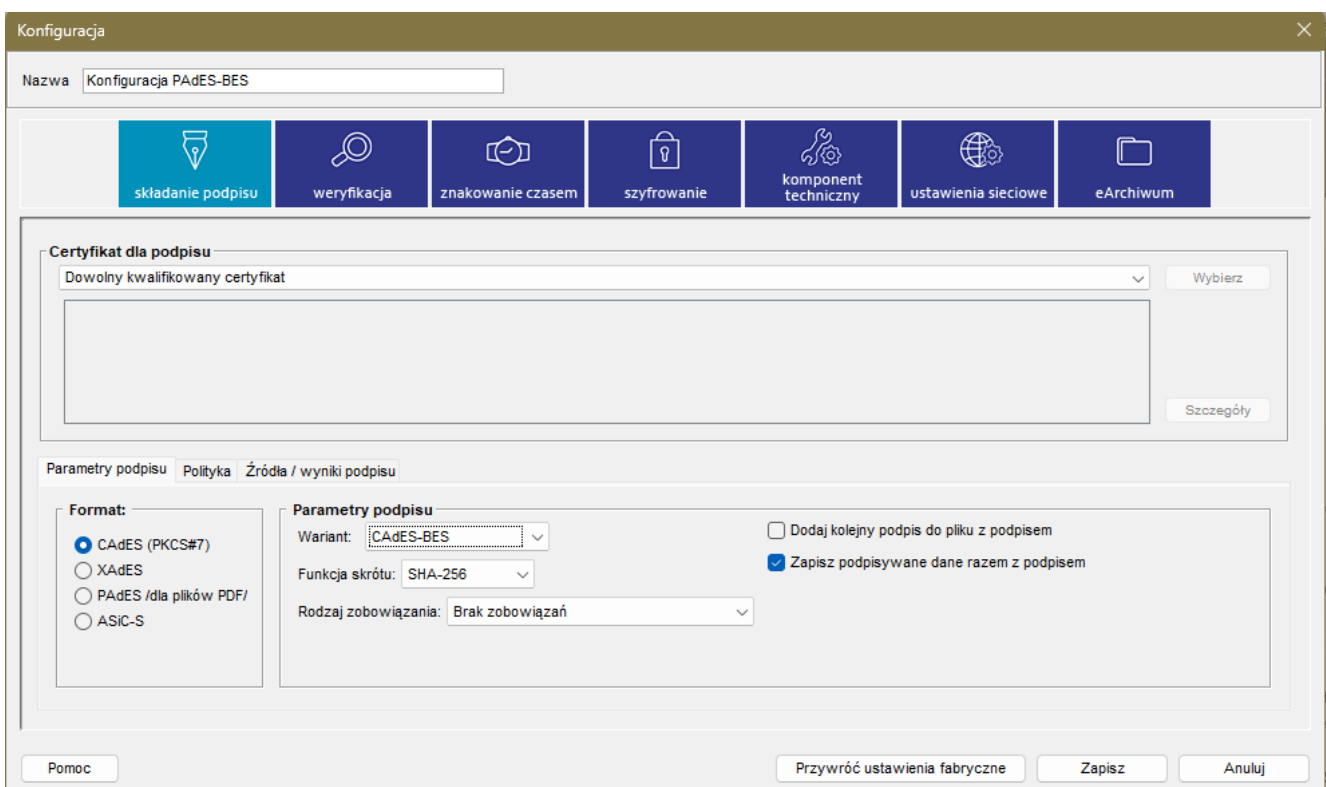
- Jeżeli dane są poprawne, **plik request.pem można będzie przesłać do podmiotu certyfikującego w celu uzyskania kwalifikowanej pieczęci elektronicznej**

Uwaga

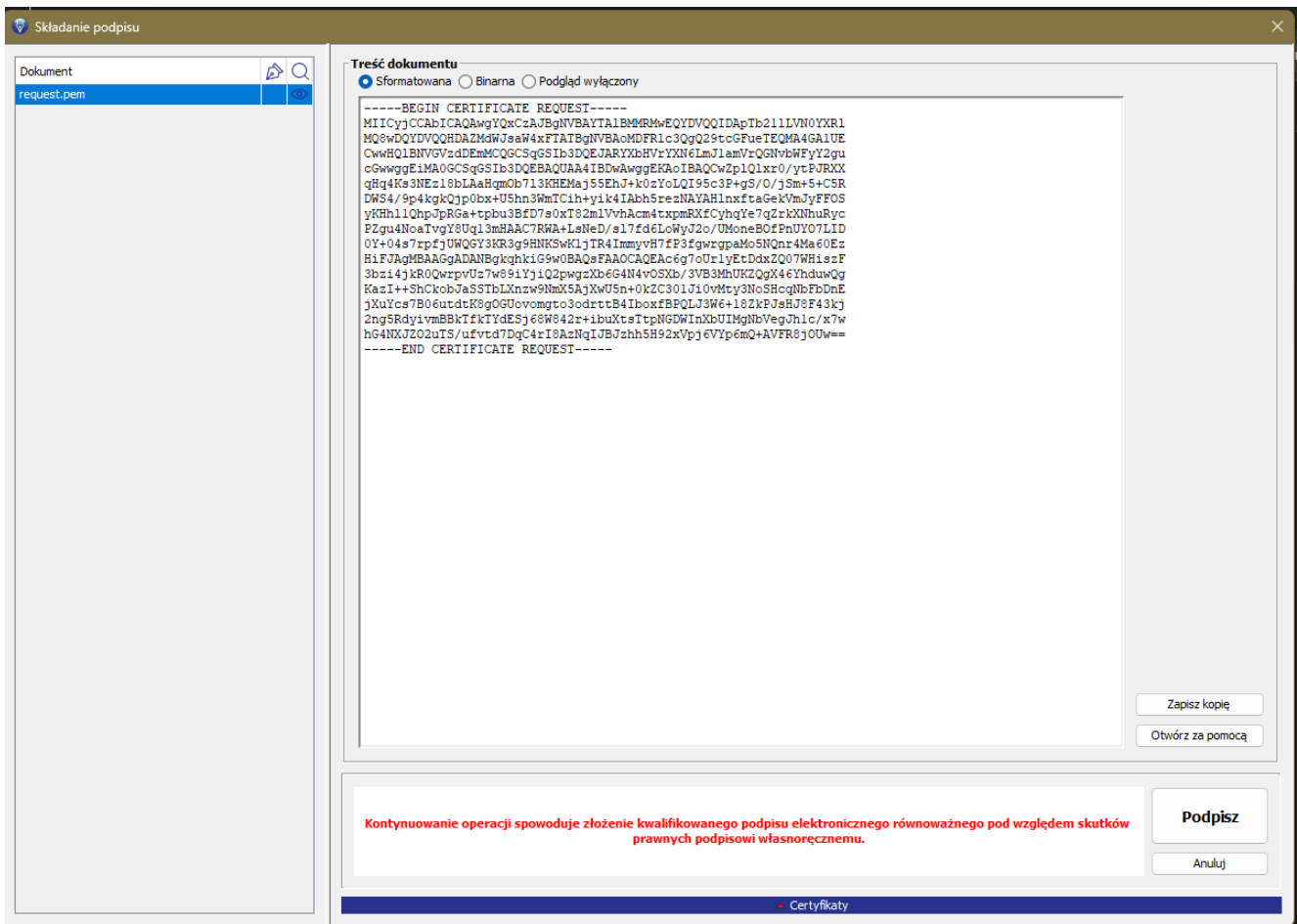
Wygenerowany klucz prywatny należy zapisać i zabezpieczyć przed dostępem osób nieupoważnionych. Klucz prywatny, w pełnej jego formie, wraz z nagłówkami i stopką, będzie niezbędny do przeprowadzenia integracji z usługą e-Doręczenia.

2. Wygenerowane żądanie CSR request.pem **przekazać do podpisu przy użyciu podpisu kwalifikowanego.**

- **Żądanie CSR (plik *request.pem*) musi być podpisane podpisem kwalifikowanym w formacie CAdES – jeśli Twoja aplikacja do podpisywania nie pozwala na złożenie podpisu w tym formacie skorzystaj z aplikacji Szafir do składania i weryfikacji podpisu elektronicznego: <https://www.elektronicznypodpis.pl/aplikacje-i-sterownik>.**
- **Składanie i weryfikacja podpisu elektronicznego w aplikacji Szafir** – w aplikacji Szafir należy kolejno:
 - przejść do sekcji **Konfiguracja**,
 - zmienić aktywną konfigurację,
 - ustawić format na **CAdES (PKCS#7)**,
 - w sekcji **Parametry podpisu** zaznaczyć opcję **Zapisz podpisywane dane razem z podpisem**,
 - zapisać konfigurację i podpisać plik żądania certyfikatu, korzystając z aplikacji Szafir,

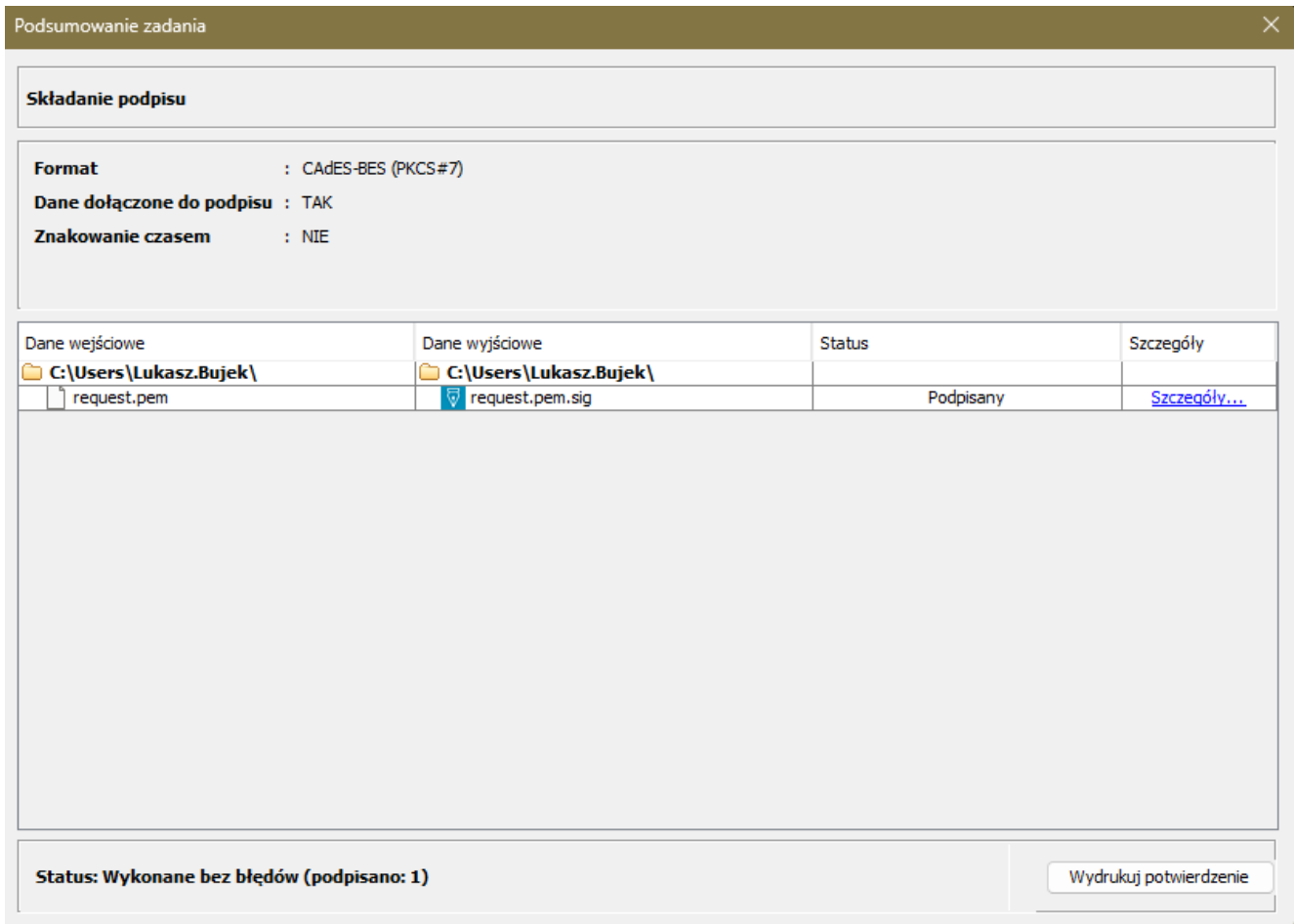


Zmiana formatu i zaznaczanie opcji „Zapisz podpisywane dane razem z podpisem” w aplikacji Szafir



Podpisywanie pliku żądania certyfikatu w aplikacji Szafir

Po podpisaniu żądania otrzymamy plik z rozszerzeniem **.sig**, który będzie można przekazać do KIR.



Okno aplikacji Szafir po podpisaniu żądania – w polu „Dane wyjściowe” widoczny jest plik z rozszerzeniem sig

3. przejść do sklepu Krajowej Izby Rozliczeniowej i odszukać produkt *Pieczęć elektroniczna Szafir*. Można skorzystać z tego [linku](#).

- Na stronie sprzedawcy konieczne jest **wybranie terminu ważności kwalifikowanej pieczęci elektronicznej**. Dostępne opcje to: 1 rok lub 2 lata.
- Należy **wybrać właściwą dla swojej organizacji wersję pieczęci wśród wymienionych poniżej**:
 - **Pieczęć elektroniczna kwalifikowana z wgraniem żądania CSR online**:
 - **Rozwiązanie wymaga posiadania kwalifikowanego podpisu**, który jest

niezbędny do podpisania żądania CSR związanego z certyfikatem. Dzięki temu sprawę można załatwić w pełni **online**.

- Jeżeli żądanie CSR zostało wygenerowane, wówczas powinno zostać podpisane podpisem kwalifikowanym Prezesa lub Prokurenta. Szczegóły procesu podpisywania znajdują się w poprzednich krokach,
- **Pieczeńć elektroniczna z dostarczeniem żądania CSR do placówki KIR:**
 - **Żądanie nie wymaga posiadania podpisu kwalifikowanego**, ale konieczna jest **fizyczna wizyta Prezesa lub Prokurenta** w jednym z dwunastu Regionalnych Centrów Sprzedaży KIR (Krajowa Izba Rozliczeniowa), aby dostarczyć wygenerowany CSR z żądaniem certyfikatu.
- Następnie należy wykonać kolejno następujące kroki:
 - **wybrać opcję Nowy zestaw**, jeśli pieczęć kupujesz po raz pierwszy. Proszę **NIE** zaznaczać opcji **Certyfikat do PSD2**.
 - **kliknąć Dodaj do koszyka**,
 - **przejsć do koszyka i kliknąć Złóż zamówienie**.
 - **kliknąć Uzupełnij dane**, w kolejnym kroku **uzupełnić dane osoby upoważnionej do odebrania pieczęci elektronicznej**,
 - **przejsć** w dół do sekcji **Dane do certyfikatu pieczęci elektronicznej** i **uzupełnić dane** zgodnie z potrzebami organizacji oraz zgodnie z danymi przekazanymi w żądaniu CSR.
- Później należy przejść niżej do ostatniej sekcji:
 - **Certyfikat online: Wgram żądanie PKCS#10** – w tym kroku należy **przesłać plik CSR w rozszerzeniu .sig, który został podpisany kwalifikowanym podpisem**.
 - **Certyfikat w placówce KIR: Dostarczę żądanie PKCS#10 do placówki KIR** – w tym kroku należy **wybrać oddział, do którego zostanie dostarczone**

żądanie certyfikatu CSR.

- Następnie należy **przejsć** do kroku 2 – **Dane do zamówienia**, a następnie do kroku 3 – **Podsumowanie i płatność**. W ramach wspomnianych kroków wykonać niezbędne **działania** opisane na stronie.
- Należy **pobrać wygenerowane zamówienie wraz z umową i przekazać je do podpisu**.

Uwaga

Konieczne trzeba upewnić się, że dokumenty zostaną podpisane przez osobę reprezentującą spółkę zgodnie z KRS lub przez osobę posiadającą odpowiednie pełnomocnictwo.

- **W celu dalszej konfiguracji integracji z usługą e-Doręczenie należy przejść do artykułu [Konfiguracja współpracy Comarch BPM z usługą e-Doręczenia](#)**