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:

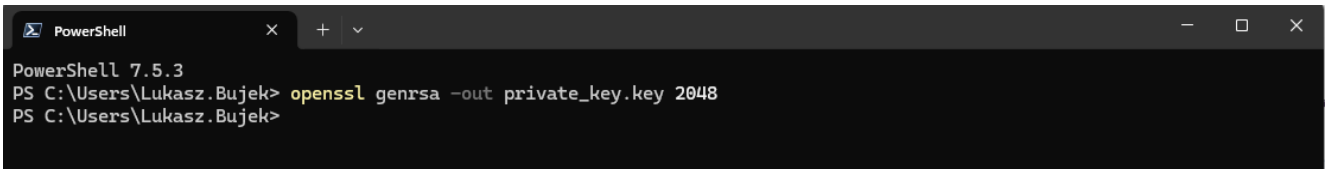
1. **Wygenerować żądanie certyfikatu CSR** – poprzez wykorzystanie

środowiska **OpenSSL**

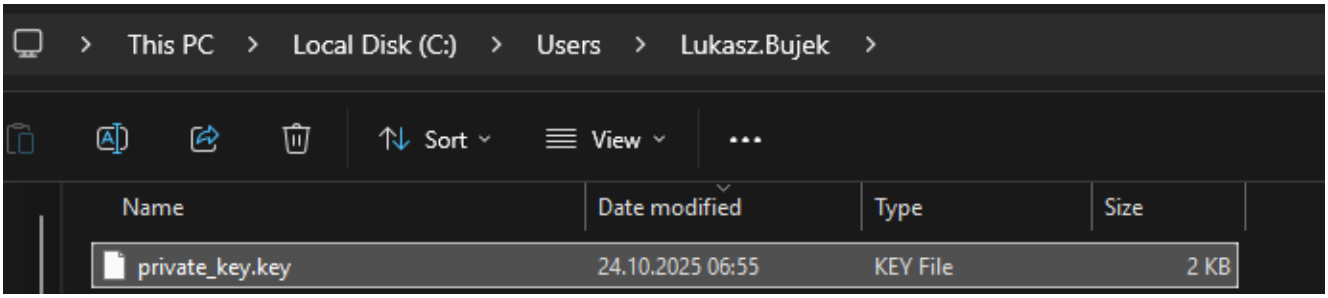
- OpenSSL to oprogramowanie open source, oferujące prosty interfejs wiersza polecenia służący do generowania kluczy. Oprogramowanie dostępne jest np. na stronie: https://slproweb.com/products/Win32OpenSSL.html
- Do przygotowania żądania CSR potrzebny będzie **klucz prywatny**:
    - Aby **wygenerować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



Wprowadzanie polecenia w terminalu



Nowoutworzony klucz prywatny o nazwie private_key.key

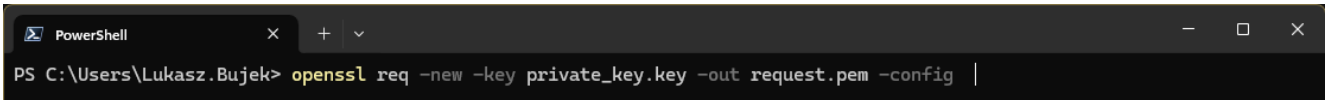
Uwaga
Plik private_key.key zostanie utworzony domyślnie w bieżącym katalogu roboczym, z którego uruchomiono polecenie.

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

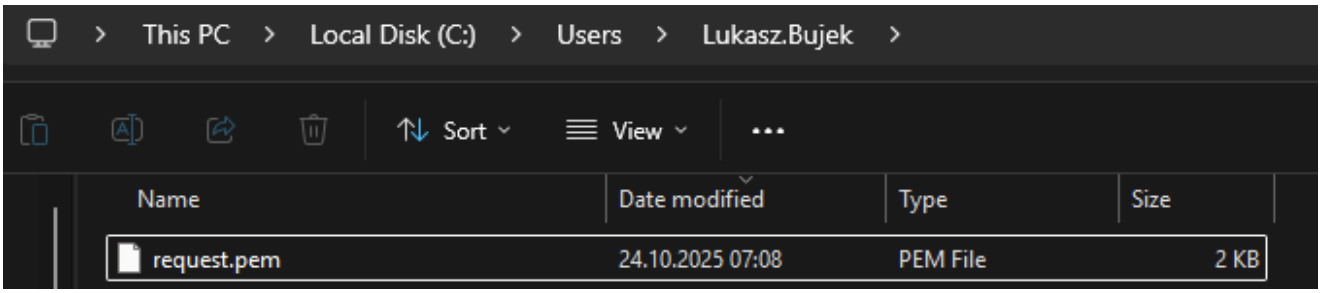
W efekcie otrzymamy **plik request.pem z zapisanym żądaniem CSR**, wygenerowany za pomocą klucza prywatnego private_key.key



Wprowadzanie polecenia w termianlu, 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).

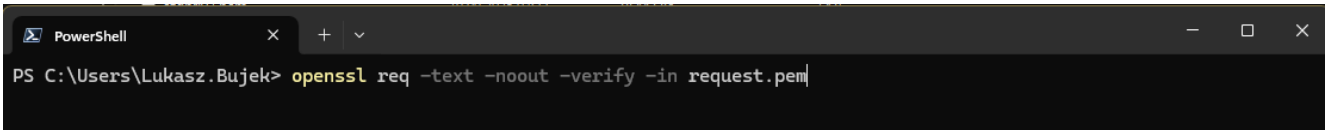


Nowoutworzone żądanie PEM

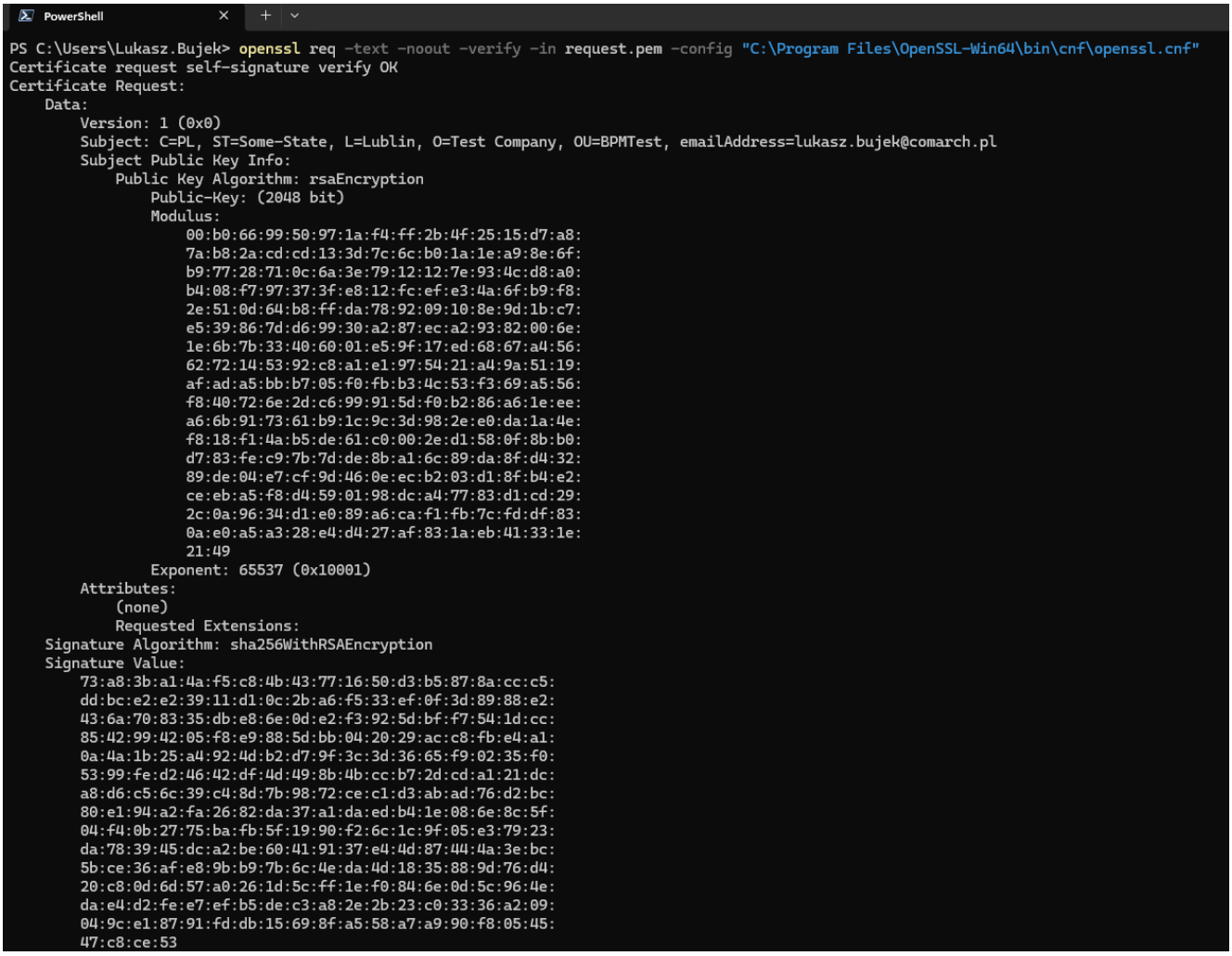
- Po utworzeniu żądania CSR można **zweryfikować** jego zawartość za pomocą polecenia:

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

Wyświetlony wynik powinien być zgodny z podanymi danymi



Wprowadzanie w terminalu polecenia weryfikującego żadanie PEM



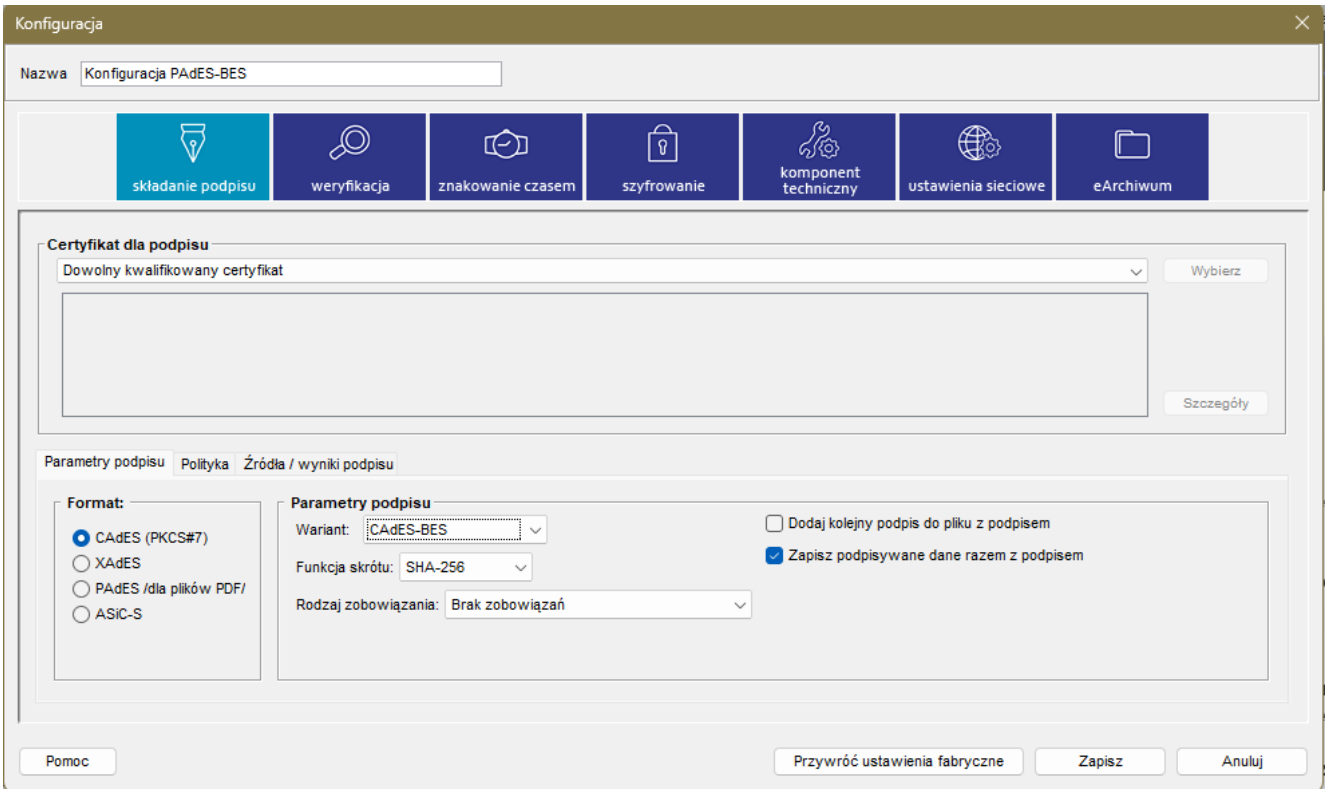
Wyniki wyświetlone po wprowadzeniu polecenia weryfikującego żadanie PEM

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

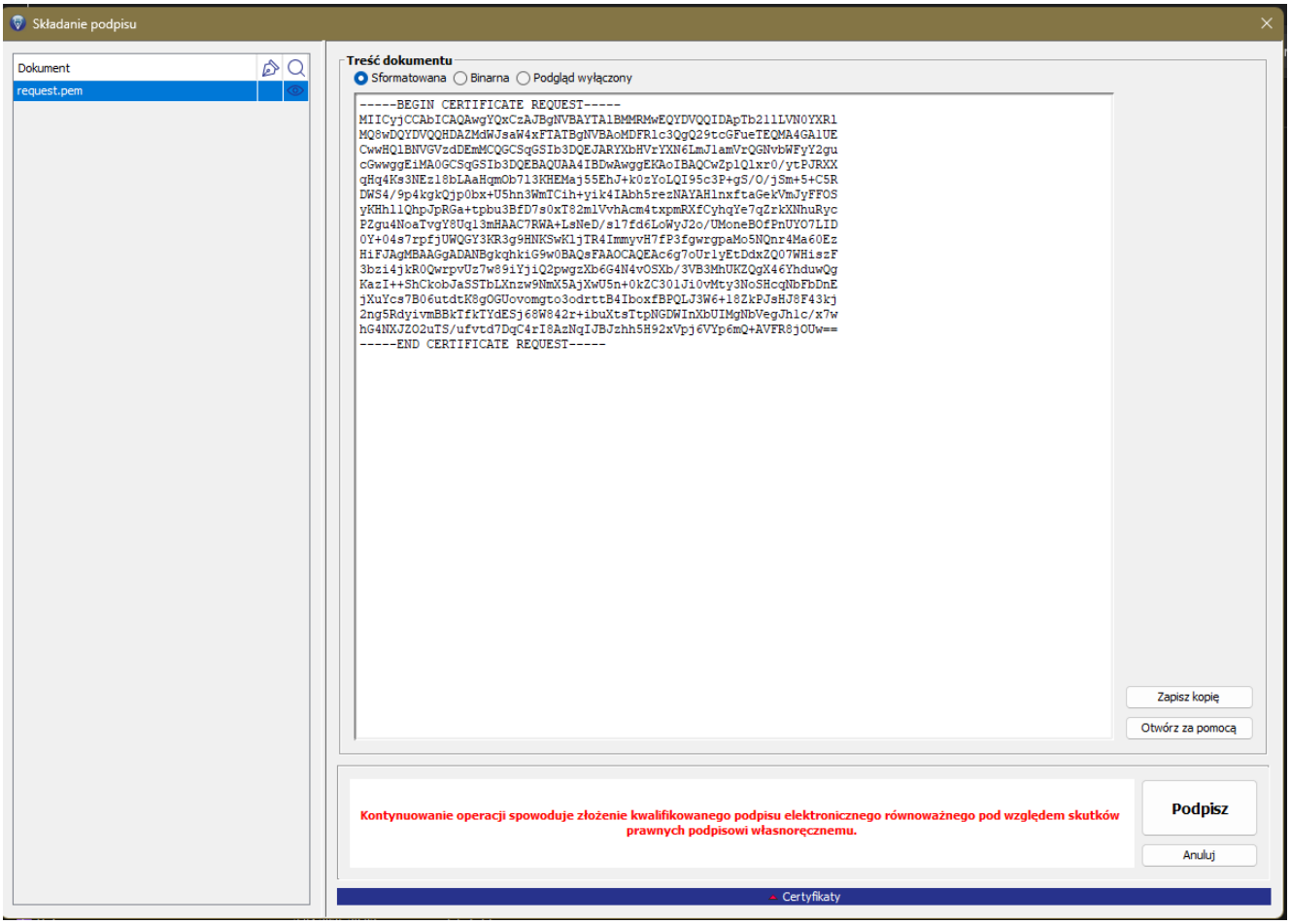
Uwaga
Wygenerowany klucz prywatny należy zapisać i zabezpieczyć przed dostępem osób nieupoważnionych. Klucz prywatny, w pełnej jego formie, wraz z nagłówkami i stopką, będzie niezbędny do przeprowadzenia integracji z usługą e-Doręczenia.

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-sterowniki.
- **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**,

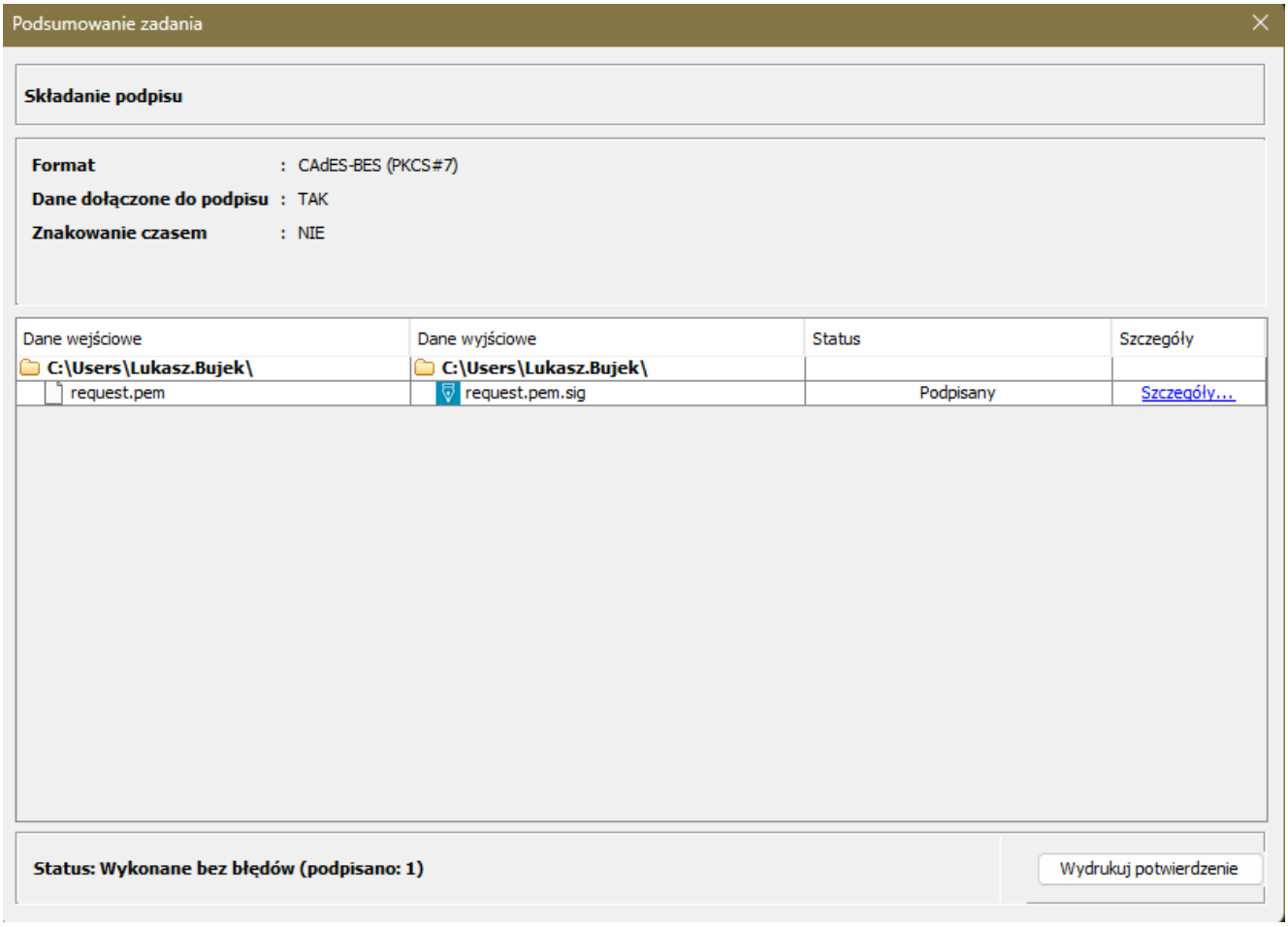


Zmiana formatu i zaznaczanie opcji *„Zapisz podpisywane dane razem z podpisem”* w aplikacji Szafir



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,
    - **Pieczęć 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.
- Nastepnie 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**,
    - **przejść do koszyka i kliknąć** **Złóż zamówienie**.
    - **kliknąć** **Uzupełnij dane**, w kolejnym kroku **uzupełnić dane osoby upoważnionej do odebrania pieczęci elektronicznej**,
    - **przejść** 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 przejść 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
Koniecznie 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**