

iRejent SignAPP

Instrukcja użytkownika



Wersja aplikacji 1.0-20260817

SoftCream Sp. z o.o. / Robert Śmietanka 2026 dla iRejent

22 sierpnia 2026 r.

1. Przeznaczenie aplikacji

SignAPP służy do podpisywania dokumentów XML kwalifikowanym podpisem elektronicznym:

- GIIF/KAS - podpis CAdES-B i szyfrowanie certyfikatem publicznym GIIF/KAS.
- PCC/SD - podpis XAdES deklaracji PCC i SD.
- Usługi CC - pobranie deklaracji, podpisanie i odesłanie do systemu CC.

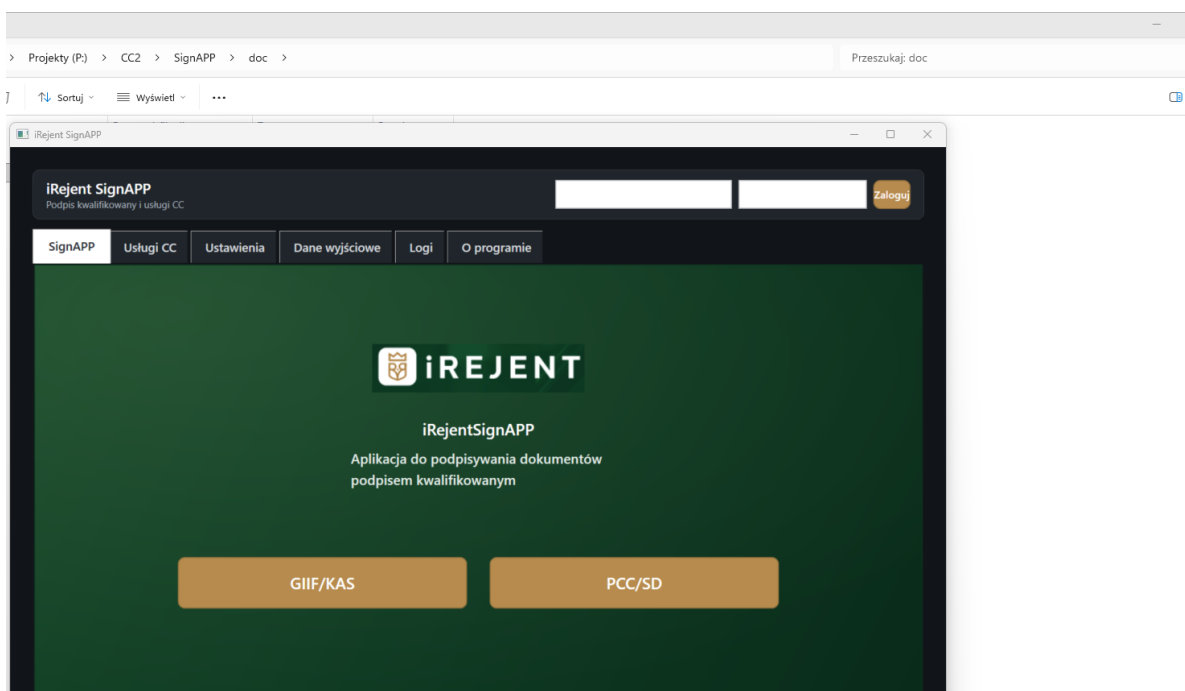
Ważne: aplikacja nie zapisuje hasła do CC. PIN wpisuj wyłącznie w oknie sterownika karty.

2. Wymagania

1. Windows i wymagany .NET Desktop Runtime.
2. Zainstalowany sterownik karty kryptograficznej.
3. Podłączona karta z ważnym certyfikatem kwalifikowanym.
4. Dla GIIF/KAS - aktualny publiczny certyfikat szyfrujący.
5. Dla CC - sieć i włączona integracja w ustawieniach.

3. Ekran główny

Zakładki główne to SignAPP, Usługi CC, Ustawienia, Dane wyjściowe, Logi i O programie. Panel logowania CC znajduje się w prawym górnym rogu.

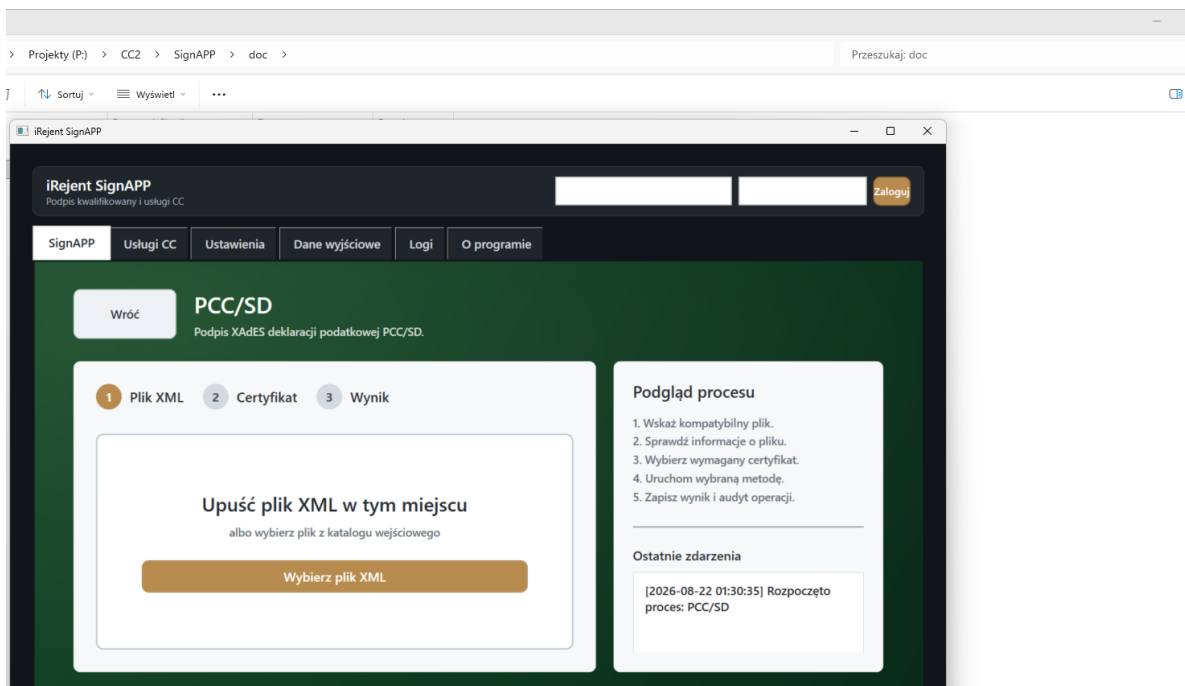


Rys. 1. Ekran startowy i wybór metody podpisu.

4. Podpisywanie pliku lokalnego

4.1. Wybór metody i pliku

1. W zakładce SignAPP wybierz GIIF/KAS lub PCC/SD.
2. Przeciągnij XML na pole wyboru albo kliknij Wybierz plik XML.
3. Sprawdź nazwę, rozmiar i podgląd. W razie pomyłki wybierz Zmień plik.



Rys. 2. Wybór pliku XML w procesie PCC/SD.

4.2. Certyfikat i podpis

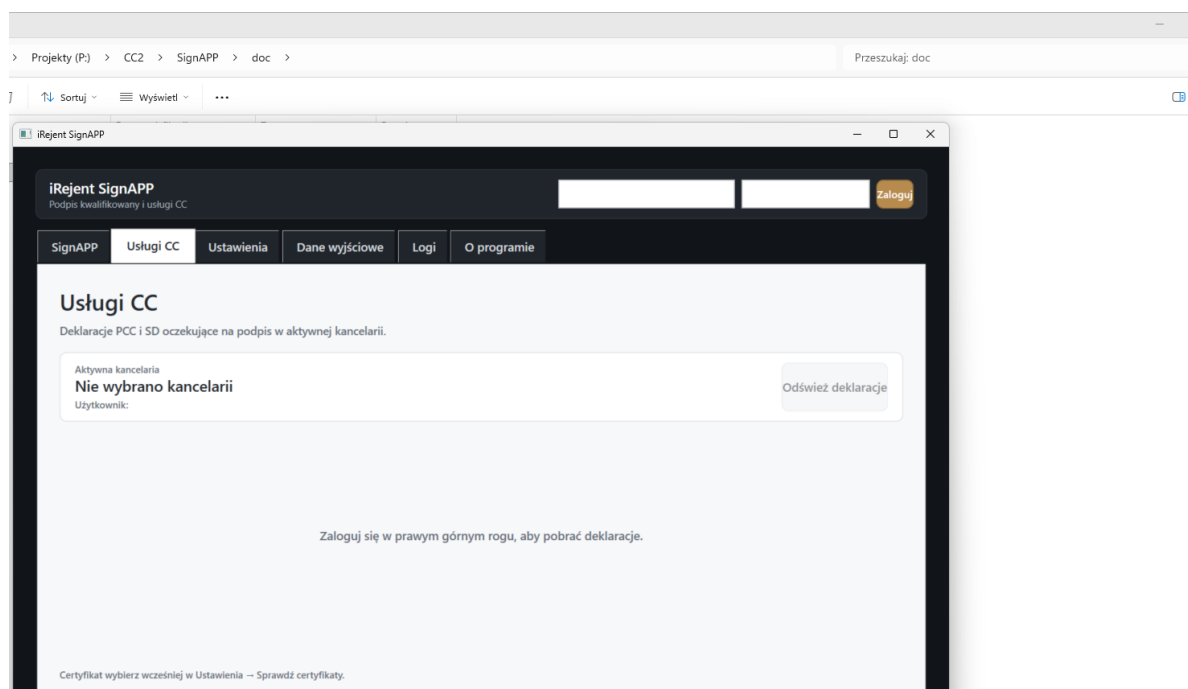
1. Przejdź do kroku Certyfikat i wybierz certyfikat kwalifikowany.
2. Sprawdź podmiot, wystawcę i termin ważności.
3. Wybierz Podpisz i podaj PIN w oknie sterownika.
4. Nie wyjmuj karty do końca operacji.

Pliki wynikowe: GIIF/KAS tworzy .xml.sig oraz .xml.sig.enc; PCC/SD tworzy plik .sing.

5. Podpisywanie przez CC

5.1. Logowanie

1. Wpisz e-mail i hasło w prawym górnym rogu.
2. Wybierz Zaloguj, a potem aktywną kancelarię.
3. Otwórz Usługi CC i wybierz Odśwież deklaracje.



Rys. 3. Usługi CC przed zalogowaniem.

5.2. Podpisanie zadania

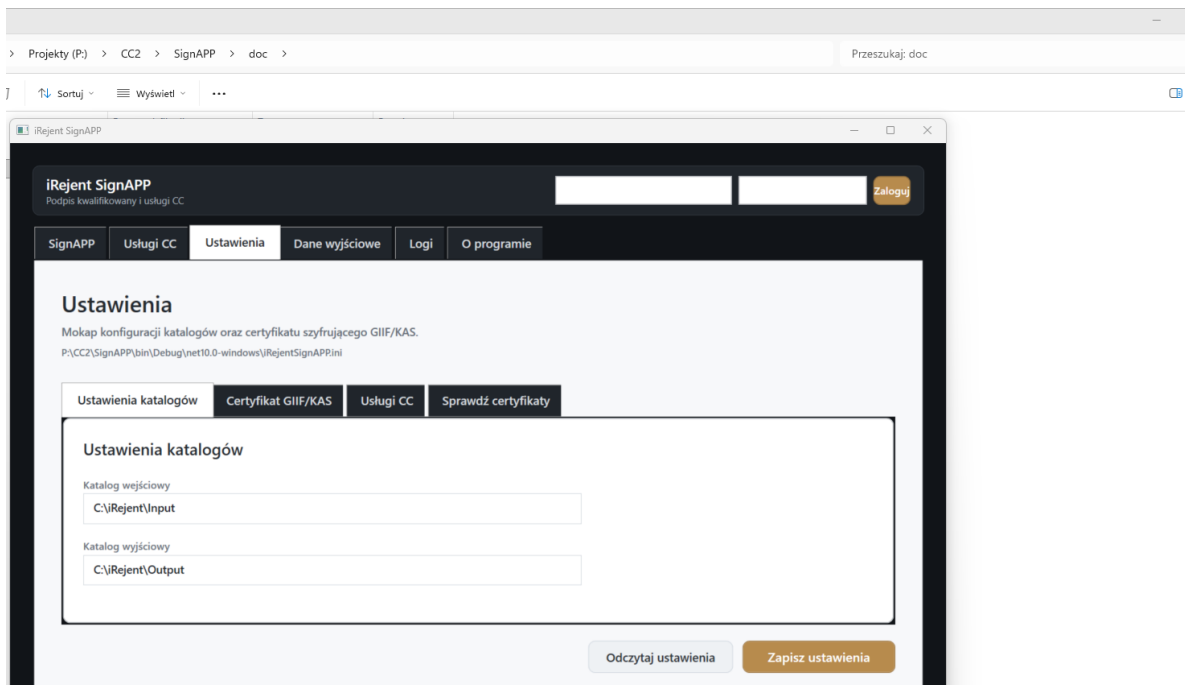
1. Wybierz PCC albo SD i sprawdź dane deklaracji.
2. Upewnij się, że wcześniej wybrano właściwy certyfikat.
3. Uruchom podpisanie następnej deklaracji i potwierdź operację.
4. Poczekaj na pobranie, podpisanie i odesłanie XML.
5. Sprawdź Dane wyjściowe i Logi; po pracy wybierz Wyloguj.

Konta wymagające 2FA nie są obsługiwane w tej wersji.

6. Ustawienia

6.1. Katalogi

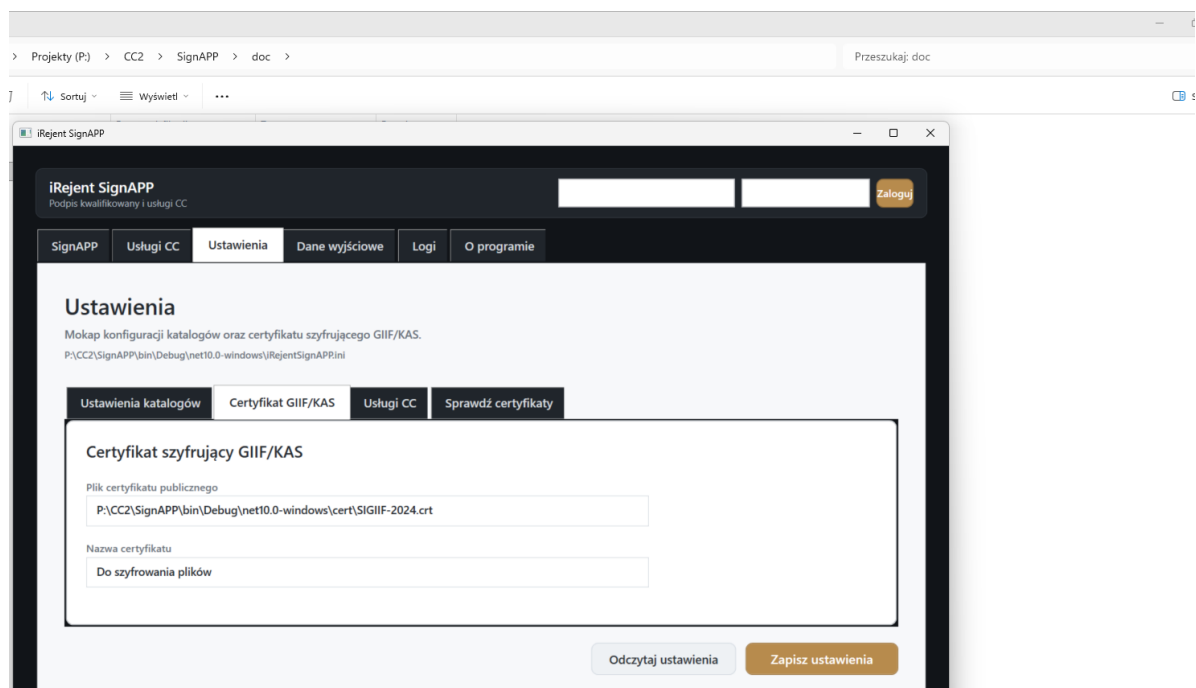
Ustaw katalog wejściowy i wyjściowy. Wybierz Zapisz ustawienia; Odczytaj ustawienia przywraca zapisane wartości.



Rys. 4. Ustawienia katalogów.

6.2. Certyfikat GIIF/KAS

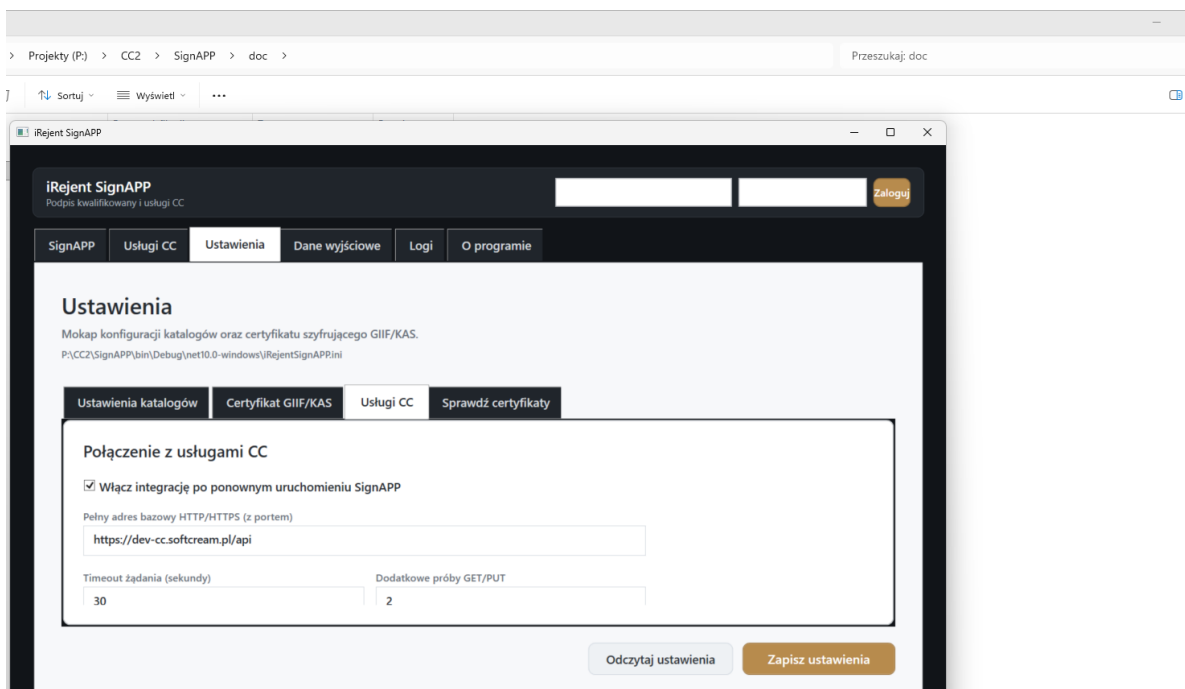
Wskaż publiczny certyfikat szyfrujący i sprawdź jego nazwę, odcisk oraz datę ważności.



Rys. 5. Certyfikat szyfrujący GIIF/KAS.

6.3. Połączenie z CC

1. Włącz integrację.
2. Podaj pełny, zweryfikowany adres bazowy HTTPS.
3. Ustaw timeout i liczbę dodatkowych prób GET/PUT.
4. Zapisz ustawienia i uruchom SignAPP ponownie.

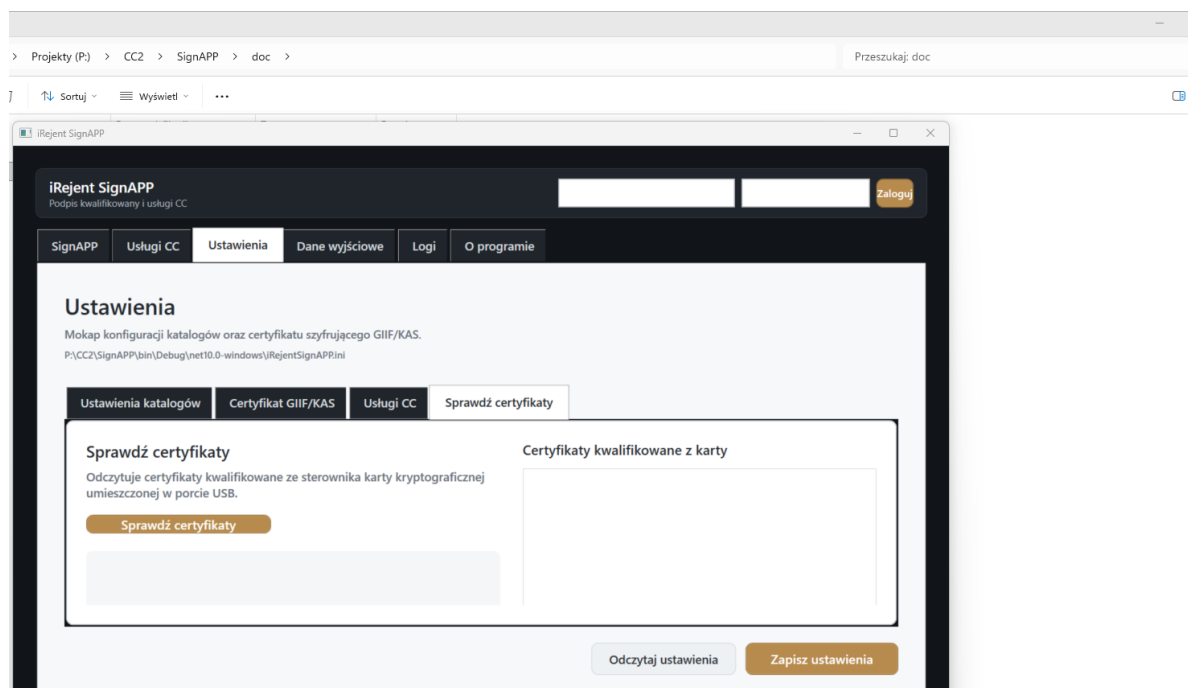


Rys. 6. Ustawienia połączenia z CC.

Adres HTTP nie szyfruje danych. Produkcja powinna używać wyłącznie HTTPS/TLS.

6.4. Sprawdzanie certyfikatów

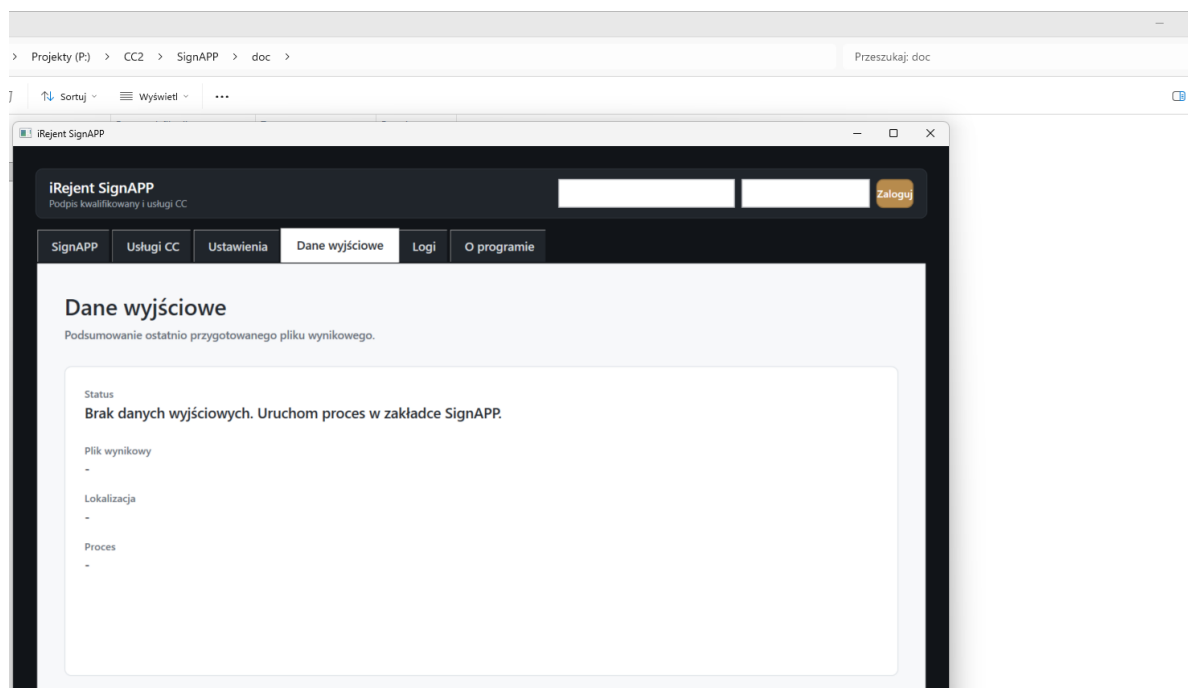
1. Podłącz kartę.
2. Otwórz Ustawienia -> Sprawdź certyfikaty.
3. Kliknij Sprawdź certyfikaty.
4. Wybierz certyfikat i zweryfikuj szczegóły.



Rys. 7. Certyfikaty kwalifikowane odczytane z karty.

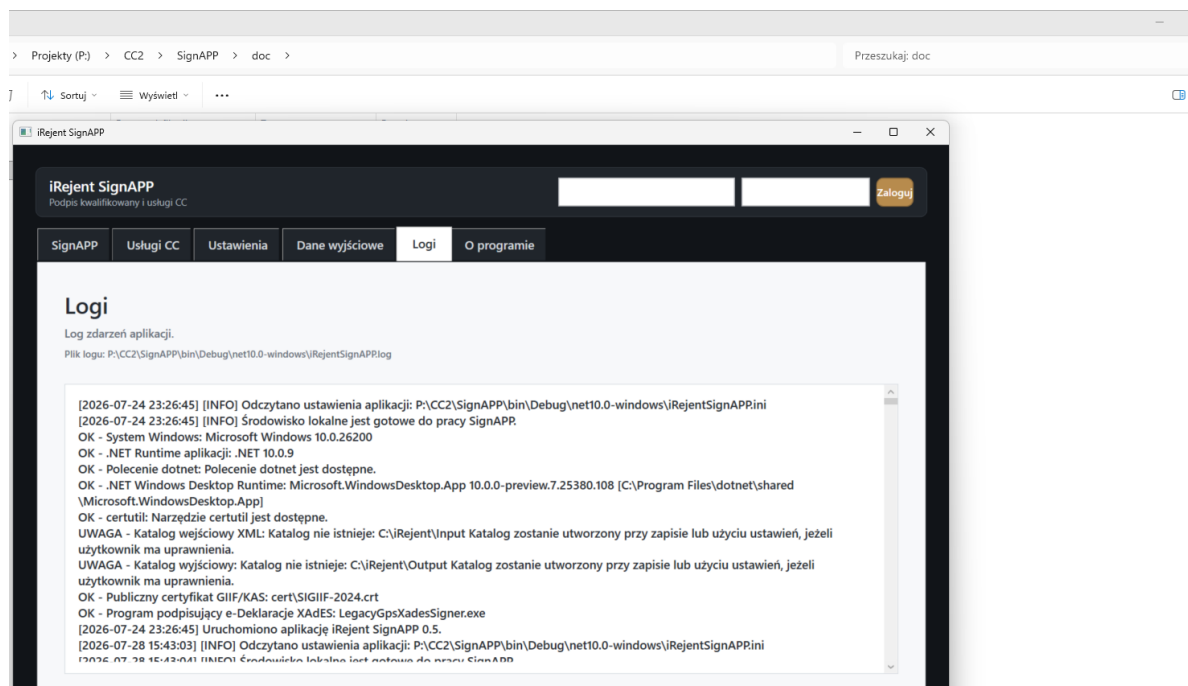
7. Dane wyjściowe i logi

Dane wyjściowe pokazują status ostatniej operacji, nazwę, lokalizację pliku i rodzaj procesu.



Rys. 8. Podsumowanie danych wyjściowych.

Logi zawierają chronologiczny zapis zdarzeń i ścieżkę do pliku logu. Przy zgłoszeniu błędu podaj komunikat oraz czas zdarzenia.



8. Najczęstsze problemy

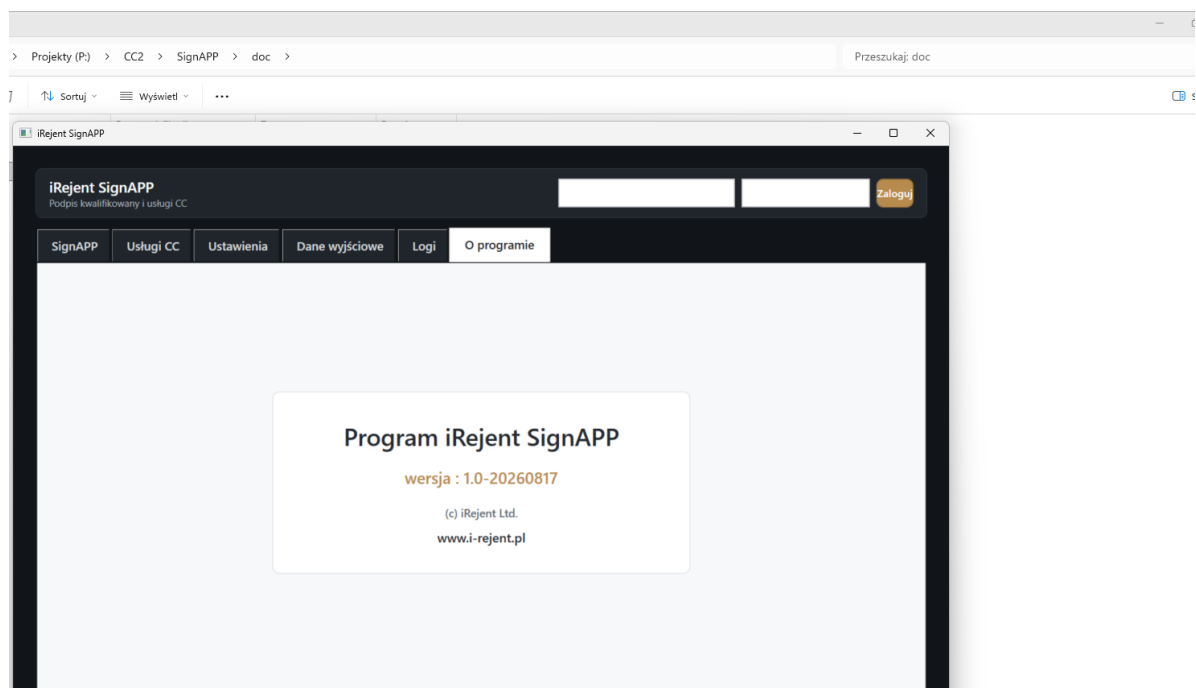
Problem	Co zrobić
Brak certyfikatu	Podłącz kartę, sprawdź sterownik i ponów skanowanie.
Podpis nieaktywny	Wybierz poprawny XML, certyfikat i katalog wyjściowy.
Błąd logowania CC	Sprawdź dane, adres usługi i sieć; 2FA nie jest obsługiwane.
Brak deklaracji	Wybierz kancelarię, odśwież listę i sprawdź PCC/SD.
Timeout / 5xx	Spróbuj ponownie; przy powtórzeniu przekaż wpis logu administratorowi.
Błąd 409/412	Odśwież listę i ponów operację na aktualnej wersji.
Nieznany wynik wysyłki	Nie podpisuj ponownie bez sprawdzenia statusu w CC.

9. Dobre praktyki bezpieczeństwa

- Sprawdź treść dokumentu i metodę przed podpisaniem.
- Nie udostępniaj PIN-u ani hasła do CC.
- Nie pozostawiaj karty bez nadzoru.
- Po pracy z CC wybierz Wyloguj.
- Nie zmieniaj ręcznie podpisanego pliku.
- Administratorowi przekazuj log i czas błędu, nigdy dane dostępowe.

10. Informacje o wersji

W zakładce O programie sprawdź wersję aplikacji. Podaj ją przy zgłaszaniu problemu.



Rys. 10. Informacje o programie i wersji.