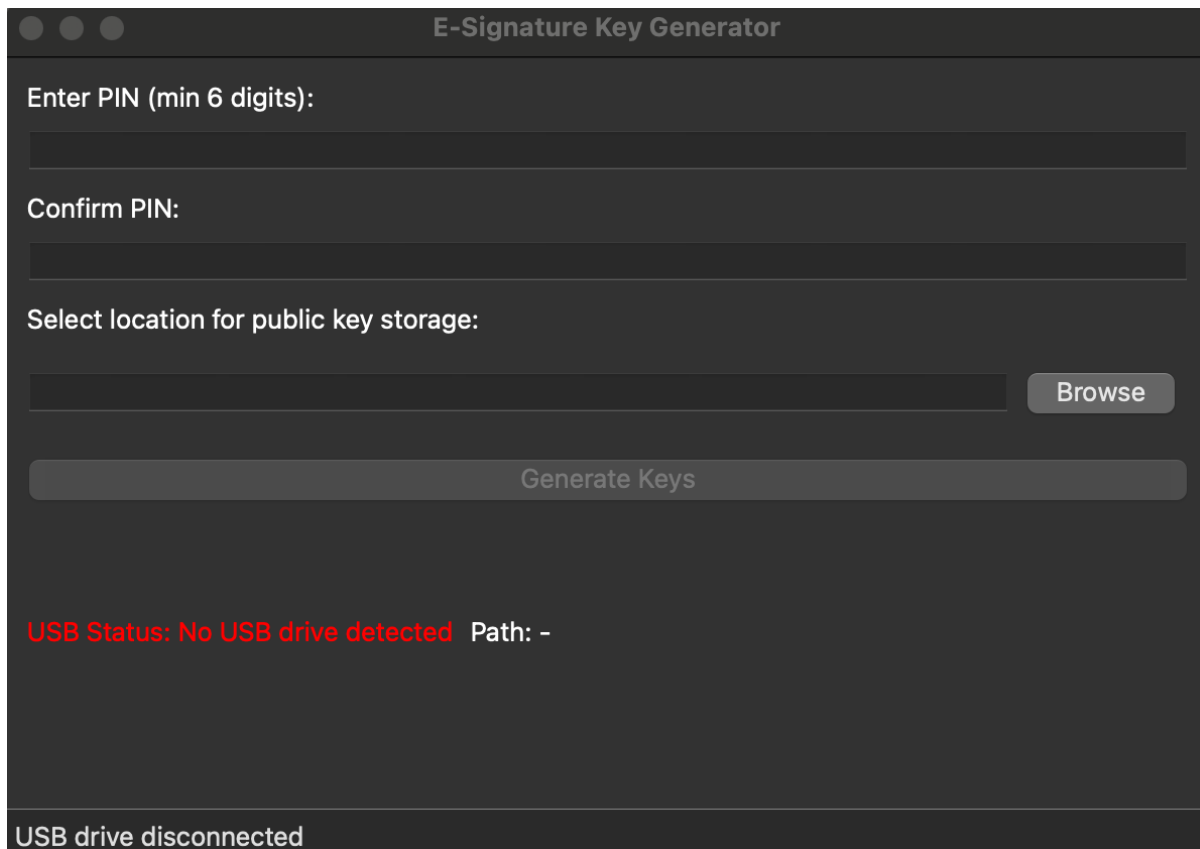


SCREENY

Mateusz Fydrych

Jan Krupiniewicz

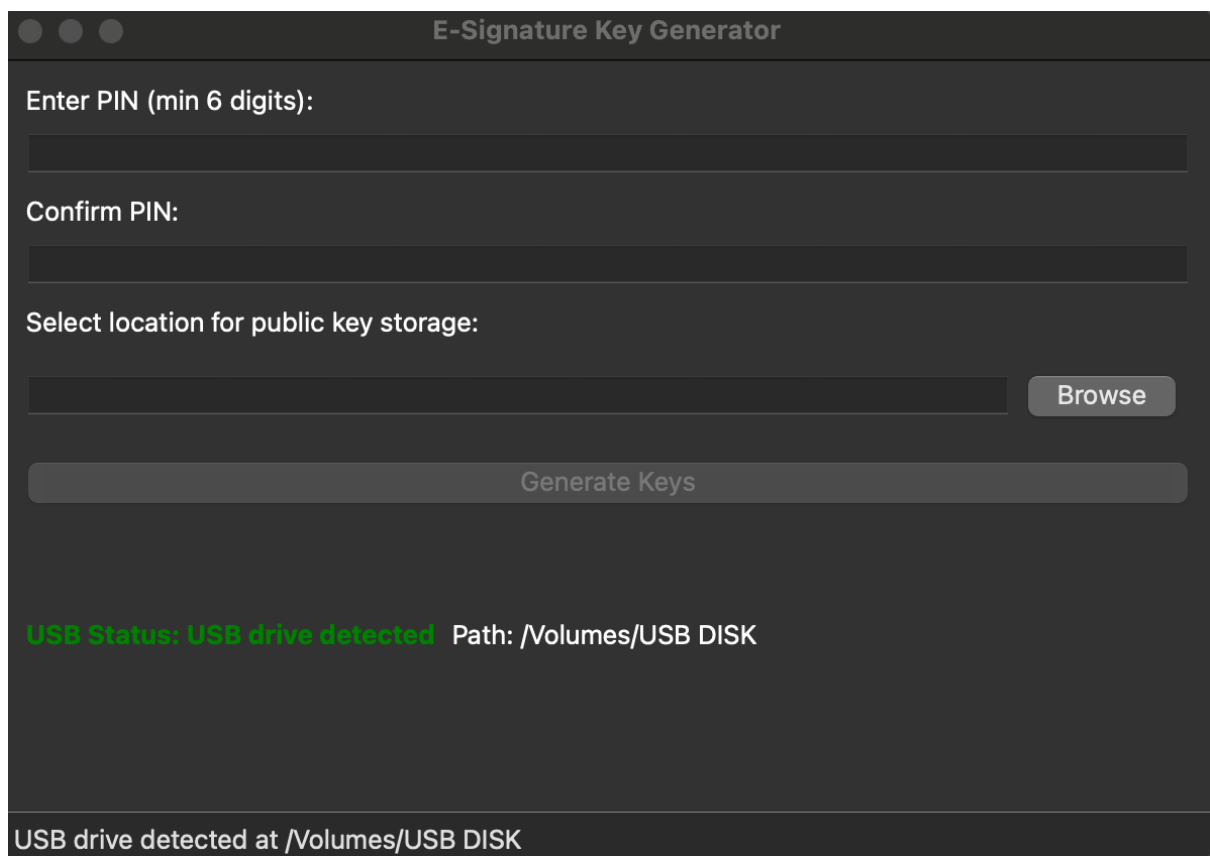
1. Aplikacja do generowania klucza



The screenshot shows a dark-themed application window titled "E-Signature Key Generator". The interface includes the following elements:

- Enter PIN (min 6 digits):** A text input field.
- Confirm PIN:** A text input field.
- Select location for public key storage:** A text input field with a "Browse" button to its right.
- Generate Keys:** A large, light-gray button.
- USB Status:** A red text message stating "No USB drive detected" followed by "Path: -".
- Footer:** A status bar at the bottom left that reads "USB drive disconnected".

Rys. 1 Podstawowa wersja aplikacji



Rys. 2 Status aplikacji po podłączeniu USB (działa również, gdy USB jest podłączone wcześniej, i dopiero wtedy się włączy aplikację.)

E-Signature Key Generator

Enter PIN (min 6 digits):

.....

Confirm PIN:

.....

Select location for public key storage:

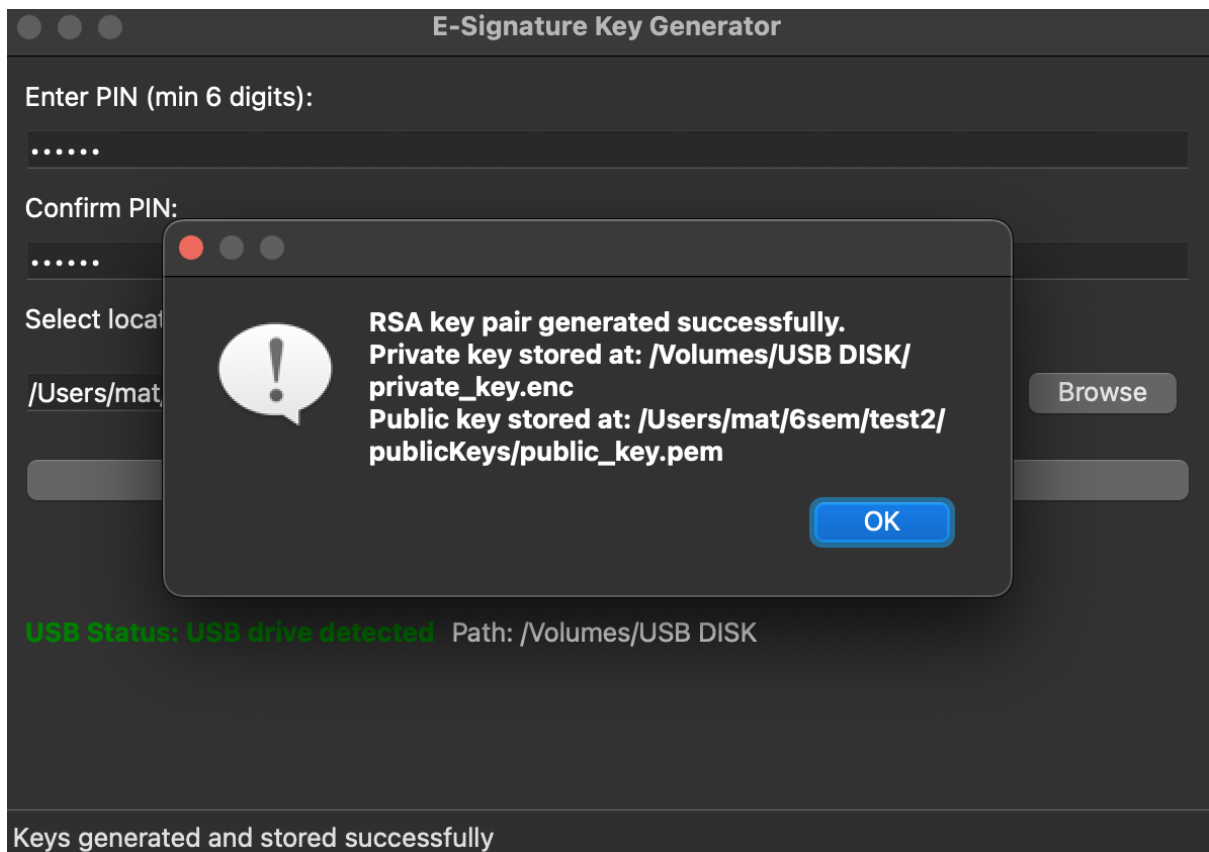
/Users/mat/6sem/test2/publicKeys Browse

Generate Keys

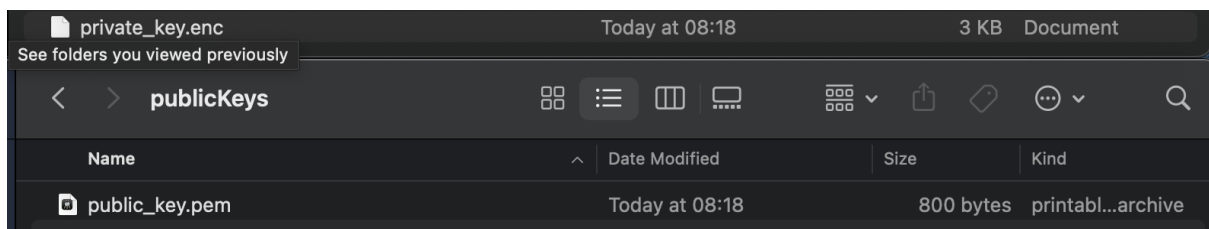
USB Status: USB drive detected Path: /Volumes/USB DISK

USB drive detected at /Volumes/USB DISK

Rys. 3 Status aplikacji, gdy zostanie wpisany dwukrotnie poprawny PIN i wybrane miejsce, aby zapisać klucz publiczny. (Warto zwrócić uwagę na możliwość kliknięcia Generate Keys)



Rys. 4 Status aplikacji po zapisaniu klucza prywatnego i publicznego



Rys. 5 Pliki zapisane poprawnie

EDGE CASE

E-Signature Key Generator

Enter PIN (min 6 digits):

.....

Confirm PIN:

.....

Select location for public key storage:

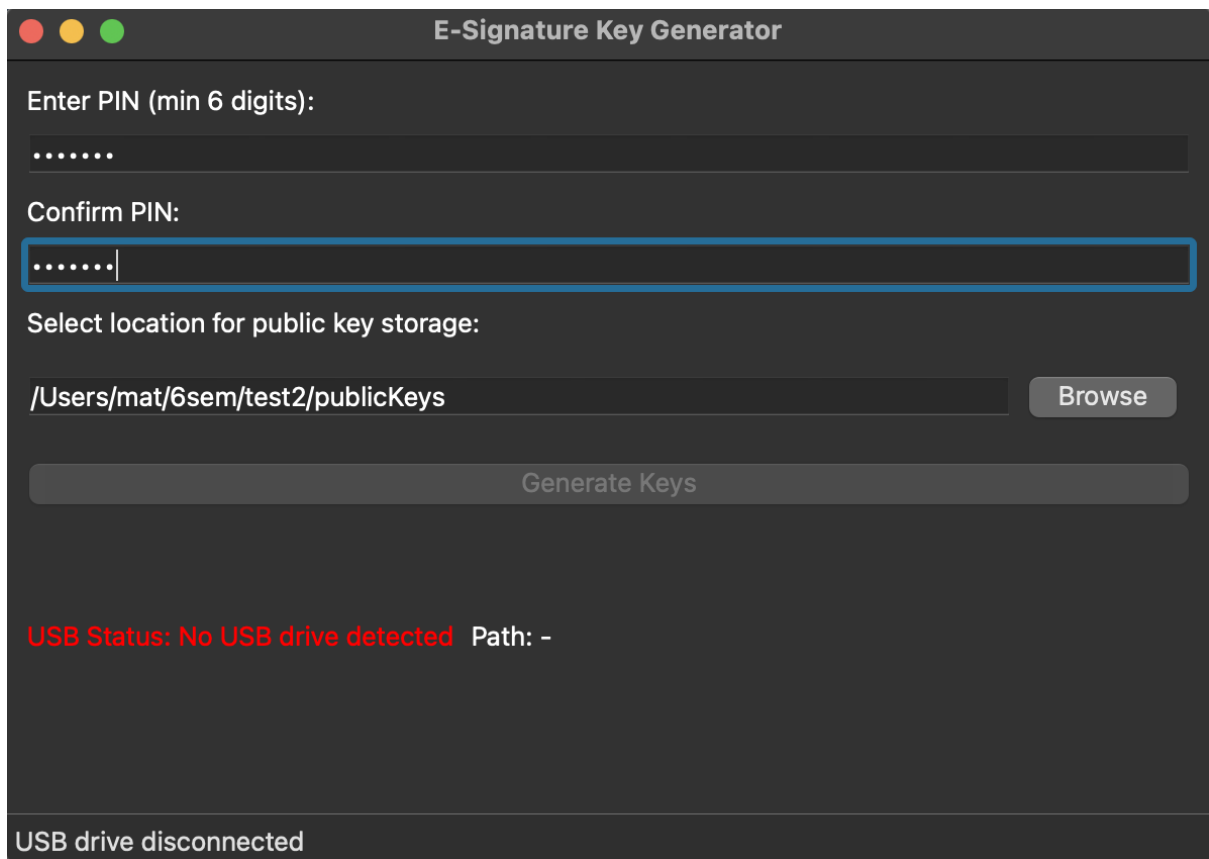
/Users/mat/6sem/test2/publicKeys Browse

Generate Keys

USB Status: USB drive detected Path: /Volumes/USB DISK

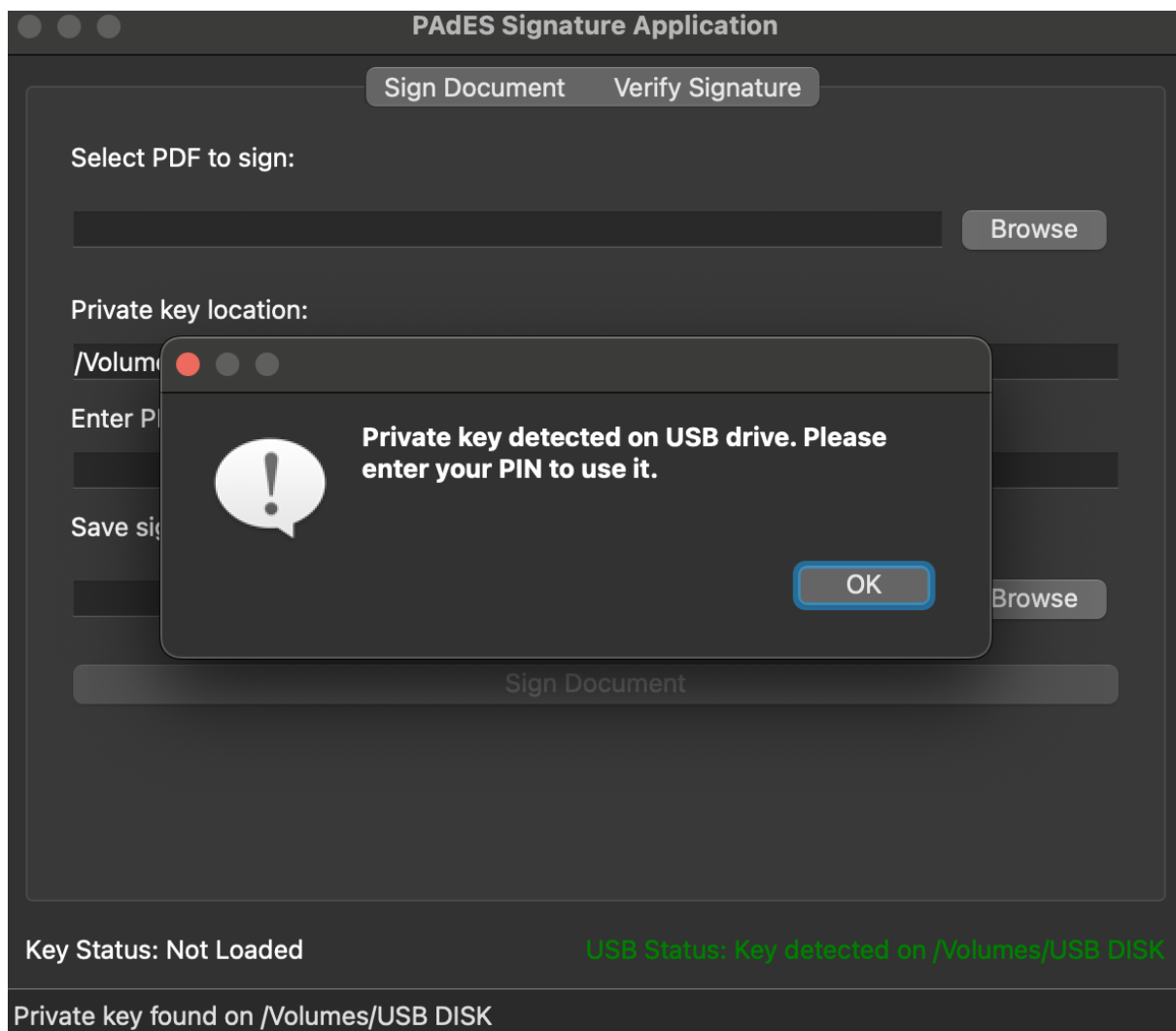
USB drive detected at /Volumes/USB DISK

Rys. 6 PINy się nie zgadzają, więc aplikacja nie pozwala na wygenerowanie kluczy

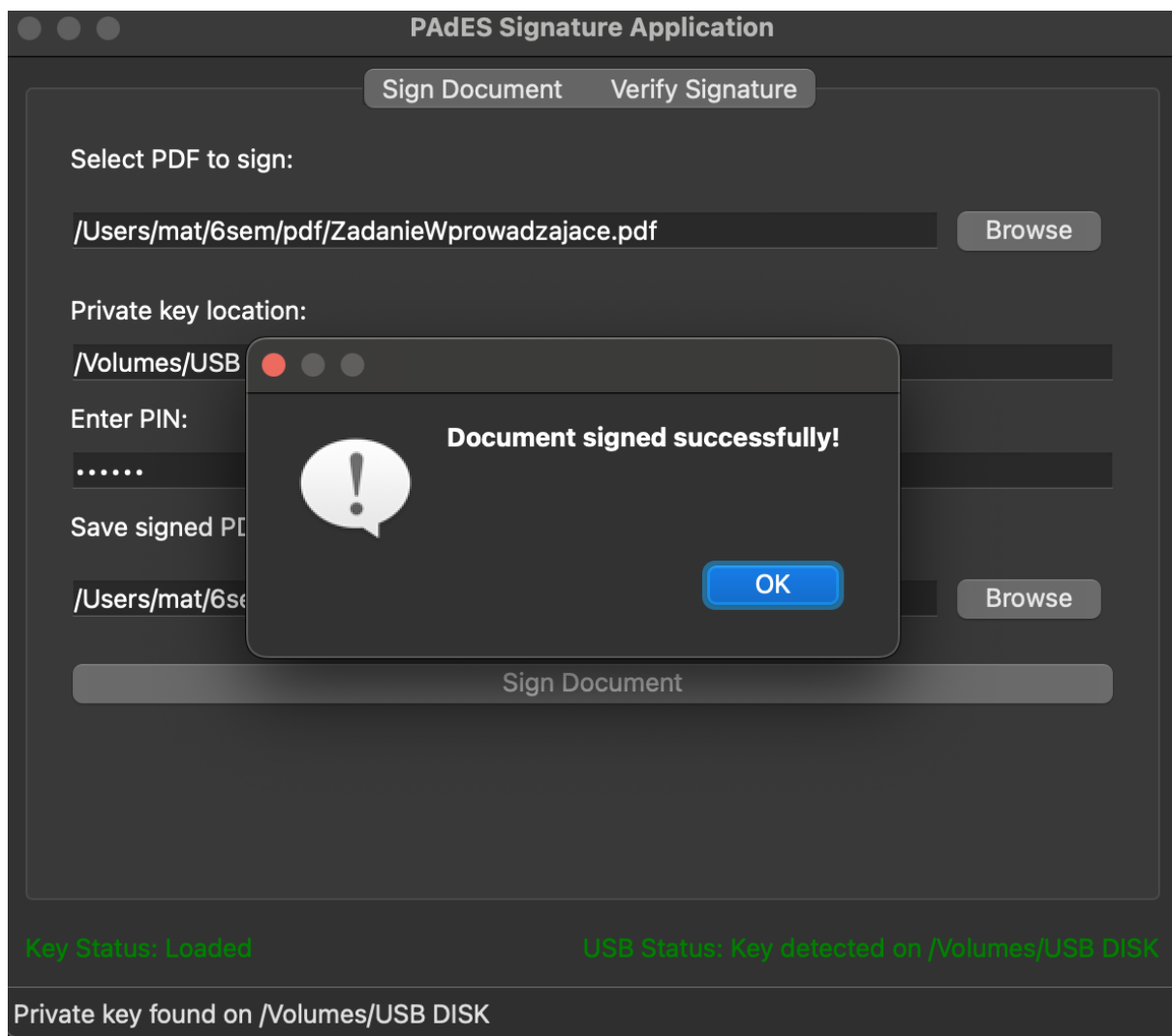


Rys. 7 USB został odłączony w trakcie (PINy się zgadzają), więc aplikacja nie pozwala na wygenerowanie kluczy

2. Aplikacja do podpisywania i sprawdzania podpisu



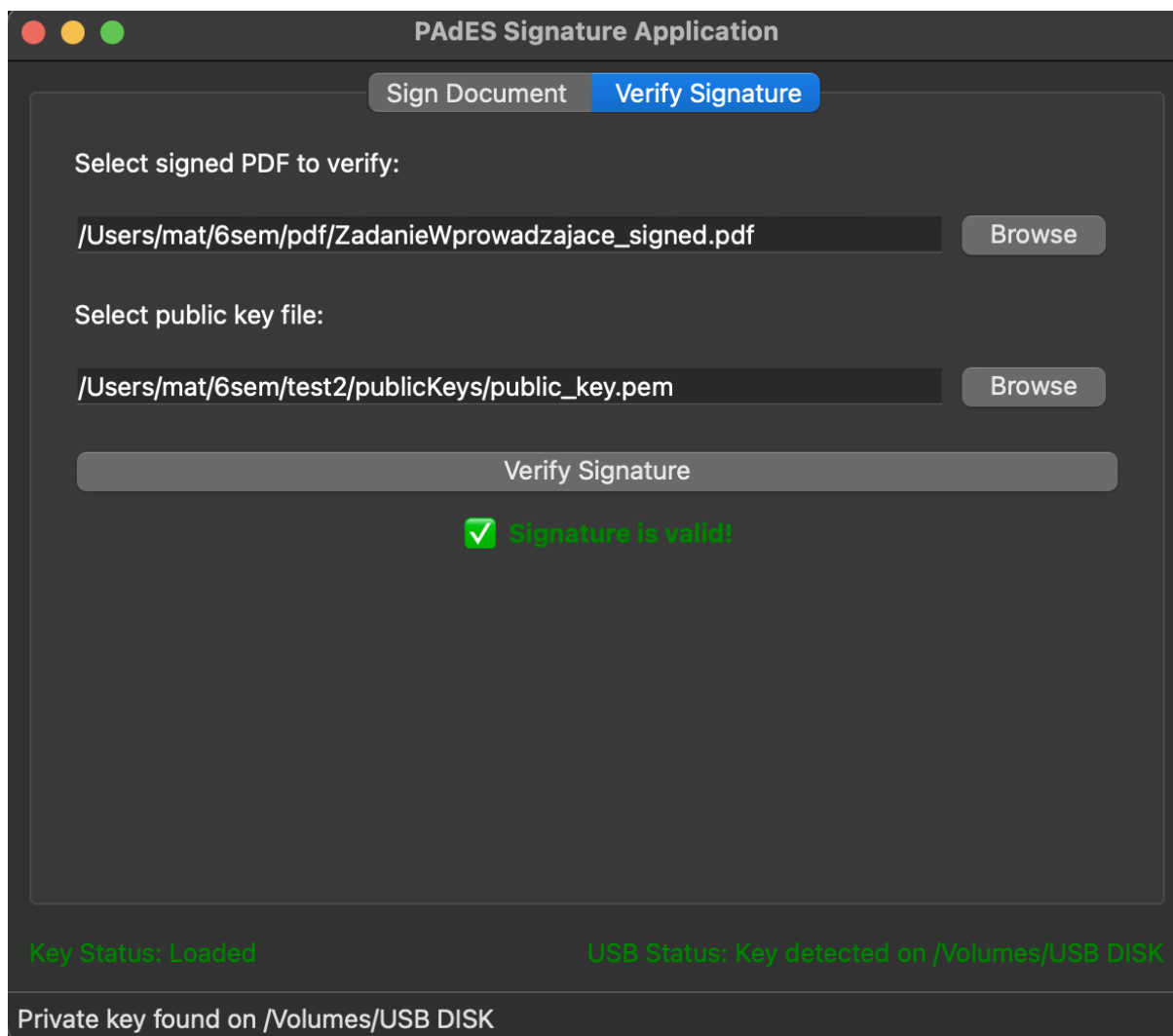
Rys. 8 Status aplikacji, gdy USB (z prywatnym kluczem) jest podłączone



Rys. 9 Status aplikacji po prawidłowym podpisaniu dokumentu

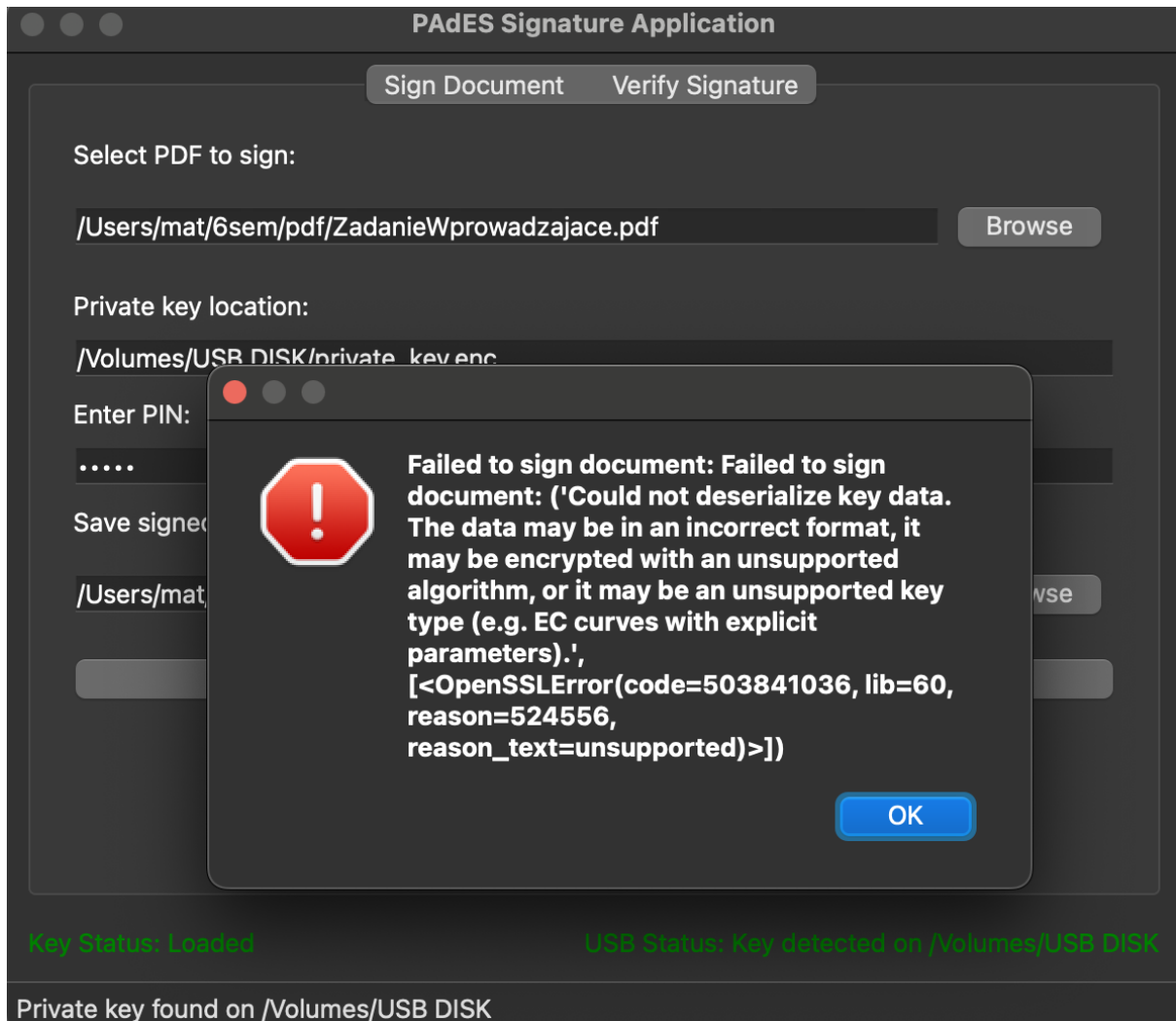

```
endobj
2 0 obj
<<
/Producer (Microsoft\256\040ffice\040Word\0402007)
/PAdES-Signature (True)
/SignatureDate (ZadanieWprowadzajace\056pdf)
/SignatureType (RSA\055SHA256)|
/Signature
(12529c9fc978e34f06fb183c5dec3f2e96abad2ad3d12785f161ddb14732a3e27dab7ffecb1030b22405a56d334d5dad5f92
366eb8512733cdae458ae6f1ce7994118554162af066765ea778caa102577fb6ba3e6dabf517b0bc1c007f859b70e6b34f682
8941e9495fa945d76fec3c49fa8593cc4320c05346d2f9a0dee3d92d1defd8495d140774a63dc0b4d7ef485cb67aa95ed2bb8
635dea62730ca3f080302fbbeed5db391a115ebdb353b800b8fe582ca9afadf2b4aa2fc3123dfad797151a192148b1b5740b3
28e6092ef8aff61c734f7ea45689b7c6707678bd4a83ac39b208d9cbc9f284d77d6131bbf20497b496ecad6b4aa3d71d5c906
a05a192ddc1db984cc094a7b7b753c9e9b9c913592d903df9819dc10607ee1facacab07bbeba75ce1379c765df552ca1cea6f
ab58c1a9012803880b406228d45c1266eccda7b4d488abd4353ebc924d1edecd45a51b196ee2880dcc7793a15f2a0b783bdbe
1ea55ba54a97ca5f1c7edad43dfb9d2b9a71144b7fc63e933142994fd7bfde2590cd17d8c2c353c33f0f27278c65c67f38e1a
d2d21f3bcf020f48d8c80699c9eb823d081b33db90b2a3936562e16f8672ebfb8a0f9c2c1b02b05d31c4bf23dd730e9bef02c
04ef5663532ff088fc15528ec28f10a86dbef62a7fe9d14c36a8fcae99c1ece00820535fe68be3ae400516372ebe99418d242
12cdd8298c30f1a)
/InitialHash (2e7fffb00f9039d96eb283da019766da82da54cf51b885a1f92705f0b12e5a699)
/Title (\040\050Digitally\040Signed\051)
/Author (ww)
/Subject ()
/Keywords ()
/Creator (Microsoft\256\040ffice\040Word\0402007)
/CreationDate (D\07220250422141044\05302\04700\047)
/ModDate (D\07220250422141044\05302\04700\047)
>>
endobj
3 0 obj
```

Rys. 10 Metadane pliku zaszyfrowanego

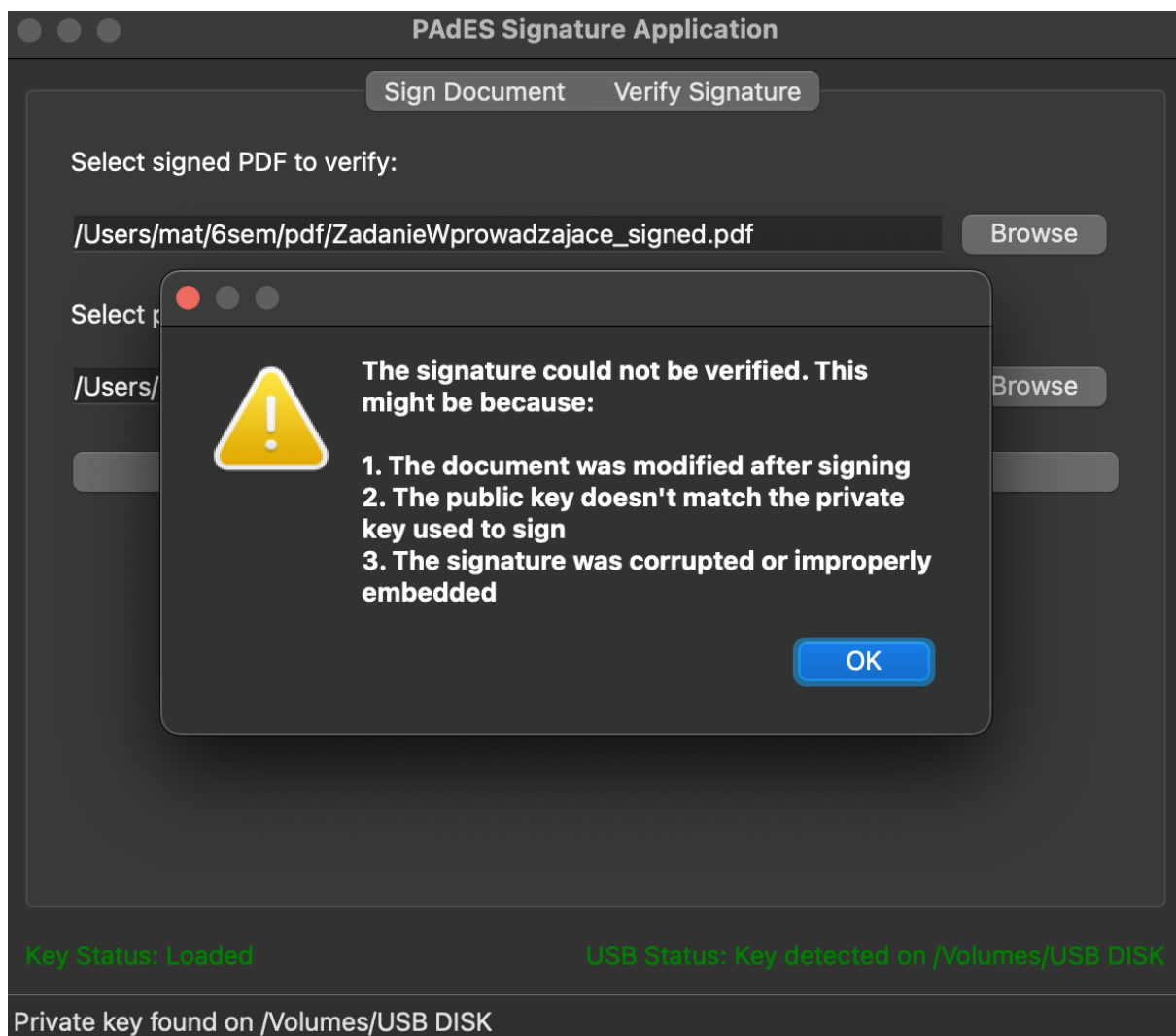


Rys. 11 Sprawdzenie prawidłowo podpisanego pliku

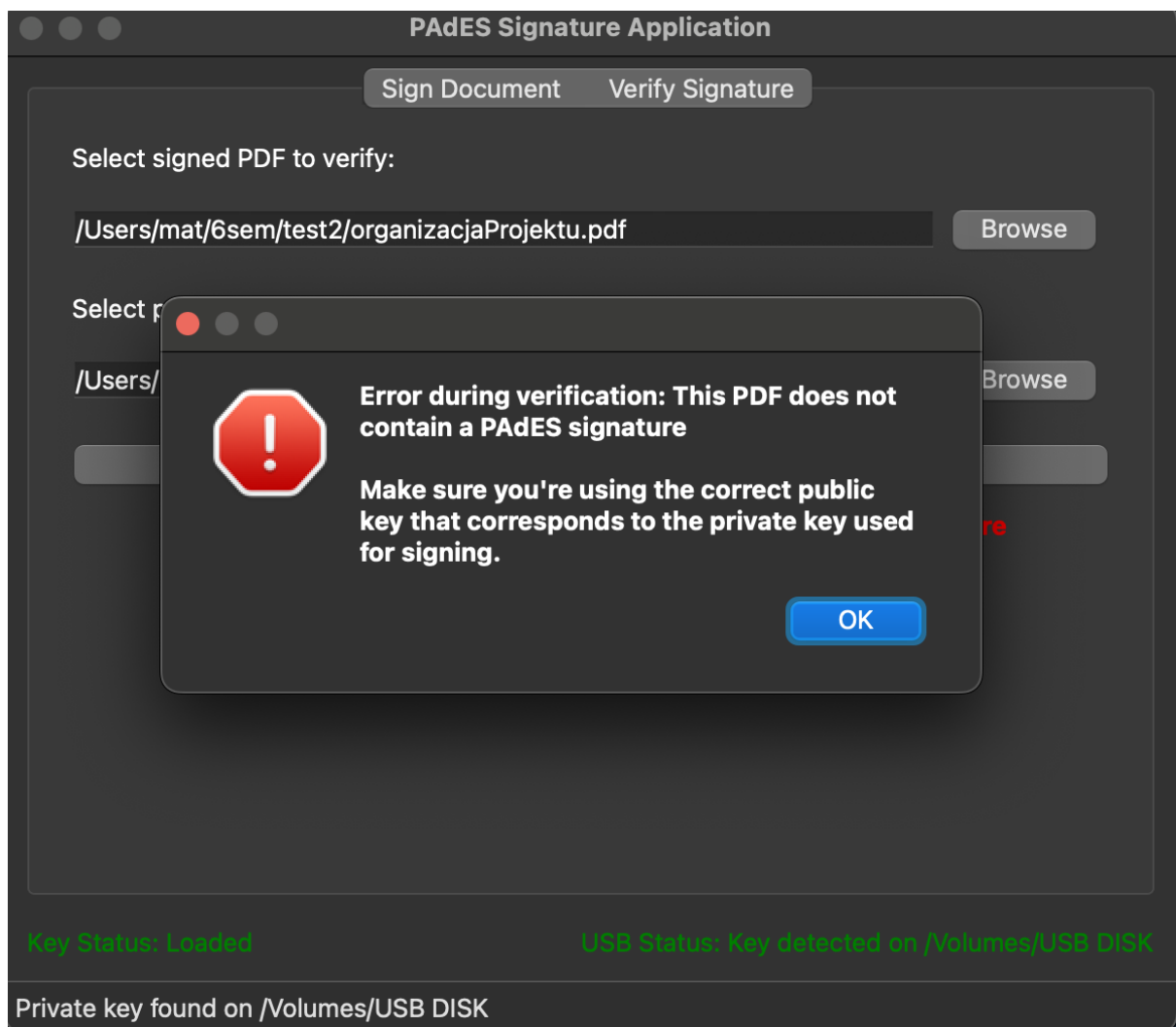
EDGE CASES



Rys. 12 Źle podany PIN podczas podpisywania dokumentu

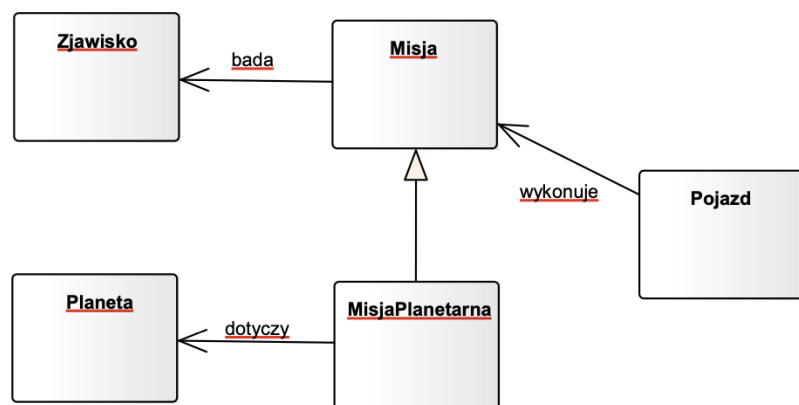


Rys. 13 Został wybrany inny klucz publiczny

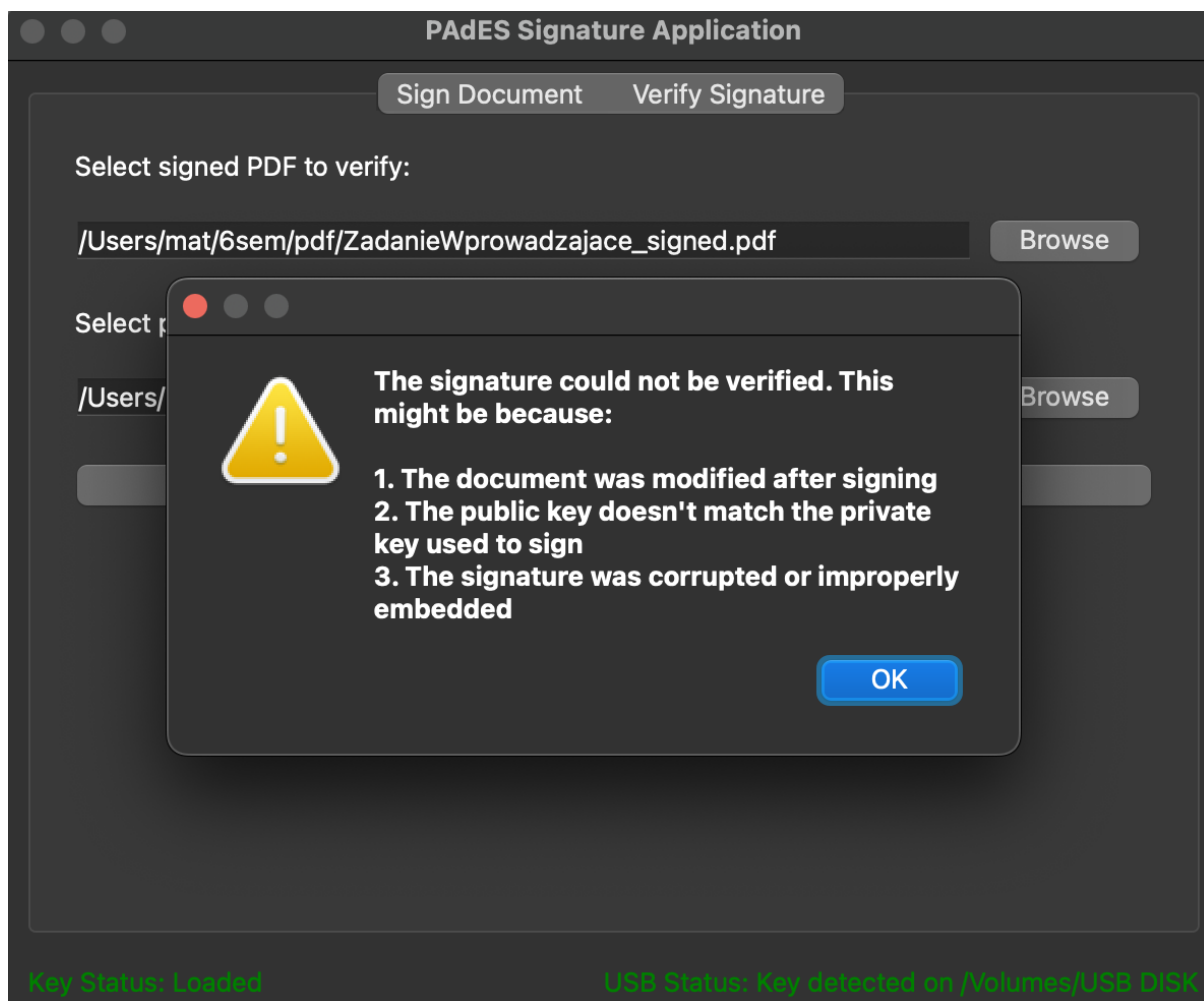


Rys. 14 Wybrany został dokument niepodpisany elektronicznie

1. Zbuduj ontologię według poniższego diagramu UML.



Rys. 15 Dorysowałem czerwone linie, czyli zmieniłem zawartość podpisanego dokumentu



Rys. 16 Przez zmianę (rys. 15), aplikacja wykryła zmianę i nie przechodzi weryfikacji.