


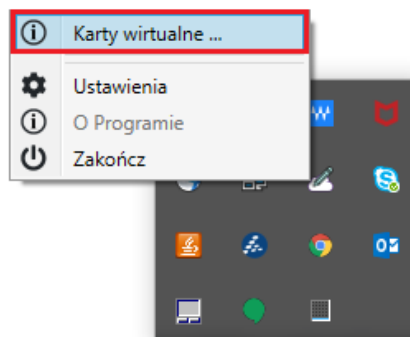
# Typowe problemy i diagnostyka aplikacji CloudSigner w systemie Windows


## Spis treści

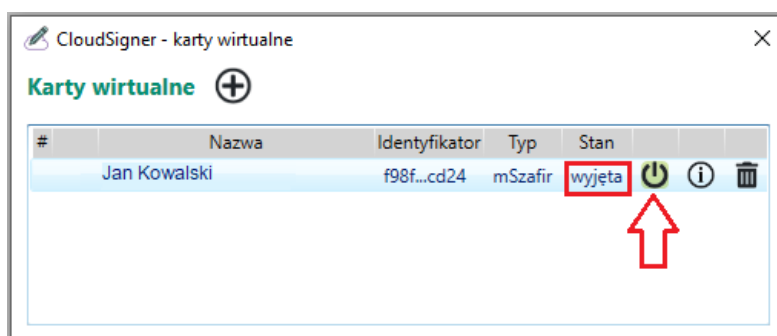
1. Problem z brakiem karty wirtualnej mSzafir w czytniku .....	2
2. Dodawanie karty wirtualnej - brak karty mSzafir .....	2
3. Brak widoczności certyfikatów mSzafir z poziomu aplikacji Szafir .....	3
4. Podpis dużej liczby dokumentów z poziomu aplikacji Szafir .....	3
5. Brak widoczności certyfikatów mSzafir z poziomu aplikacji wykorzystujących do podpisu komponenty Szafir SDK .....	5
6. W aplikacji do podpisu zamiast pytania o kod OTT, wyświetla się pytanie o PIN.....	6
7. Podpis w programie Płatnik .....	6
8. Wirtualny czytnik kart.....	8
9. Zebranie logów diagnostycznych .....	10

# 1. Problem z brakiem karty wirtualnej mSzafir w czytniku

Zweryfikuj, czy karta ma stan „w czytniku”. W tym celu najedź kursorem myszy na ikonę  CloudSigner i wybierz opcję **Karty wirtualne** z menu kontekstowego:



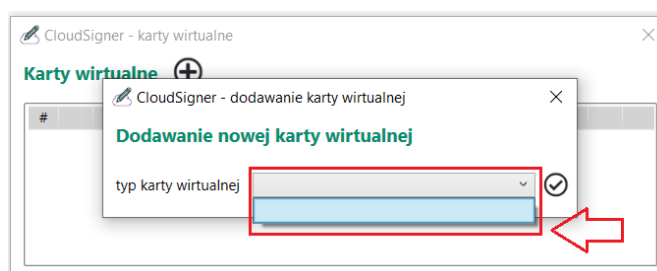
Jeśli karta ma stan „wyjęta”, najedź kursorem myszy na rekord z danymi karty i nacisnąć przycisk  :



Stan karty wirtualnej zmieni się na: „w czytniku”.

## 2. Dodawanie karty wirtualnej – brak karty mSzafir

W przypadku braku możliwości dodania karty wirtualnej mSzafir w aplikacji CloudSigner zweryfikuj połączenie z Internetem. Aplikacja CloudSigner do poprawnej pracy wymaga dostępu do Internetu na potrzeby połączenia z usługą mSzafir.



### 3. Brak widoczności certyfikatów mSzafir z poziomu aplikacji Szafir

W aplikacji CloudSigner zweryfikuj, czy karta ma stan „w czytniku”.

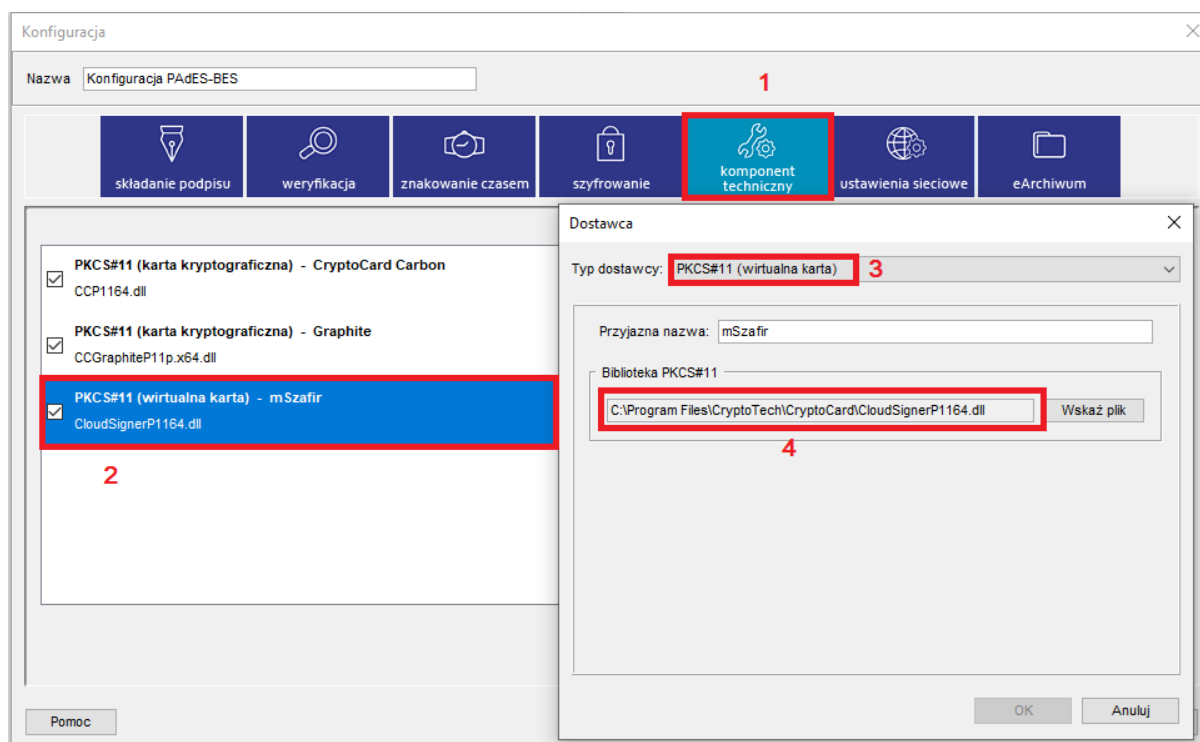
W przypadku aplikacji Szafir zweryfikuj, czy w konfiguracji komponentu technicznego zostały wskazane biblioteki PKCS#11 do obsługi wirtualnej karty mSzafir. Po instalacji aplikacji CloudSigner biblioteki znajdują się w następujących lokalizacjach:

Wersja 32 bitowa:

C:\Program Files (x86)\CryptoTech\CryptoCard\CloudSignerP11.dll

Wersja 64 bitowa:

C:\Program Files\CryptoTech\CryptoCard\CloudSignerP1164.dll



### 4. Podpis dużej liczby dokumentów z poziomu aplikacji Szafir

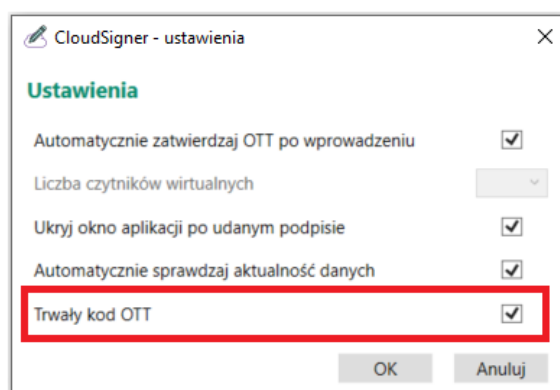
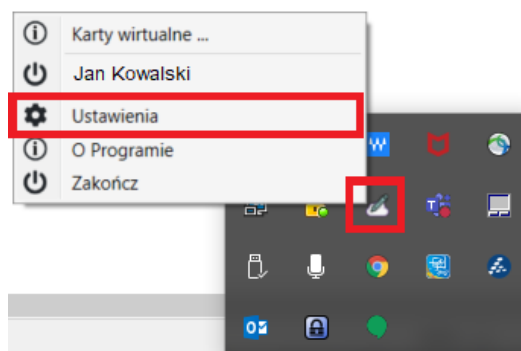
W przypadku podpisu dużej ilości dokumentów w aplikacji Szafir włącz w aplikacji CloudSigner opcję Trwały kod OTT na etapie podpisu lub w ustawieniach, dzięki czemu nie będzie konieczności podawania kodu OTT przy każdym dokumencie. Będziesz proszony o potwierdzanie kolejnych podpisów w aplikacji mobilnej w czasie ważności kodu OTT. Po tym czasie będzie poproszony o podanie nowego kodu OTT.

W tym celu:

- a. zaznacz opcję **Trwały kod OTT** na etapie podpisu



- a. lub ustaw w konfiguracji aplikacji **Trwały kod OTT**



**Uwaga:**

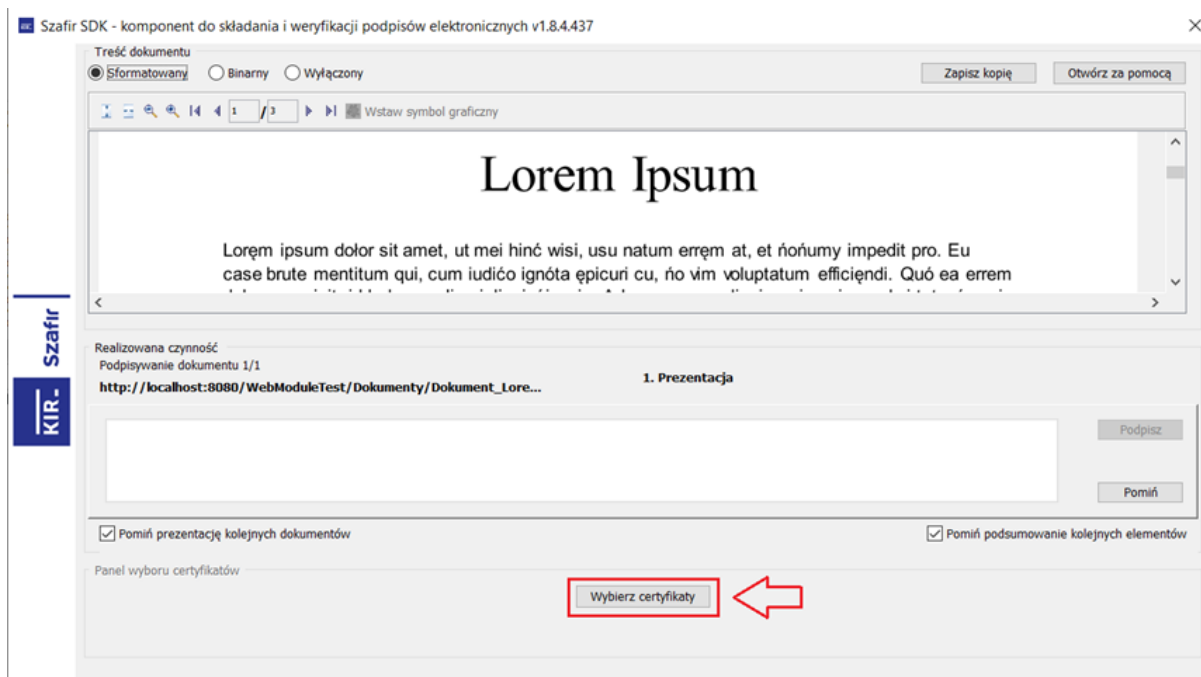
Minimalna wymagana wersja aplikacji CloudSigner wspierająca multipodpis to 1.6.2.89.

W przypadku użycia aplikacji Szafir rekomendowana jest wersja aplikacji Szafira 2.0 (build 671) lub nowsza.

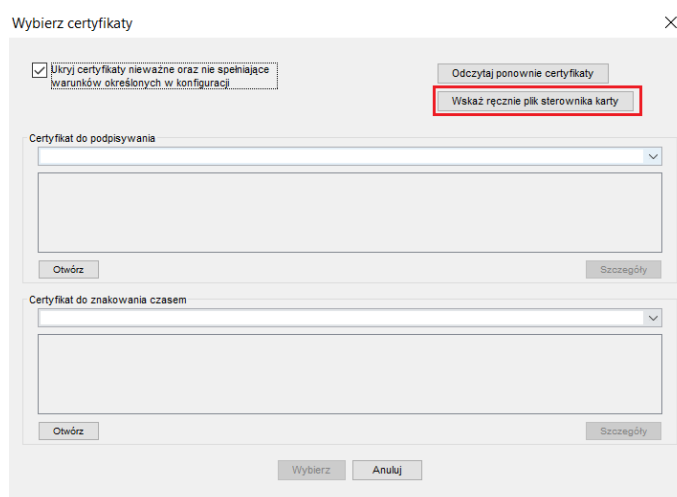
## 5. Brak widoczności certyfikatów mSzafir z poziomu aplikacji wykorzystujących do podpisu komponenty Szafir SDK

W takim przypadku wskaż samodzielnie bibliotekę do obsługi wirtualnej karty mSzafir w momencie pojawienia się okna z prezentacją dokumentu do podpisu. W tym celu:

- wybierz przycisk „Wybierz certyfikaty”



- następnie „Wskaż ręcznie plik sterownika karty”:



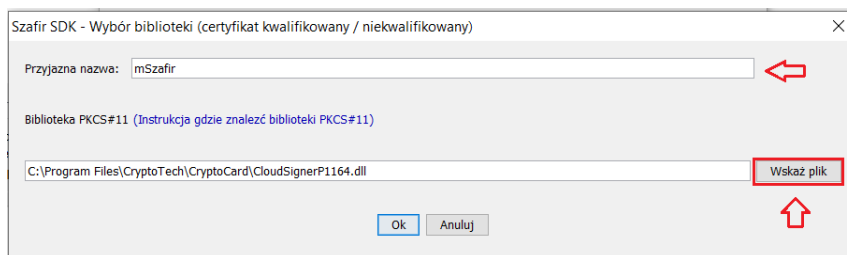
- w oknie wyboru biblioteki nadaj przyjazną nazwę i wskaż bibliotekę PKCS#11 do obsługi karty. Po instalacji aplikacji CloudSigner biblioteki znajdują się w następujących lokalizacjach:

Wersja 32 bitowa:

C:\Program Files (x86)\CryptoTech\CryptoCard\CloudSignerP11.dll

Wersja 64 bitowa:

C:\Program Files\CryptoTech\CryptoCard\CloudSignerP1164.dll



- Po kliknięciu „OK” i zatwierdzeniu wyboru biblioteki zostaniesz przekierowany do okna wyboru certyfikatu. W tym momencie certyfikaty mSzafir zostaną automatycznie odczytane, zaprezentowane i będą mogły zostać użyte do podpisania dokumentów.

## 6. W aplikacji do podpisu zamiast pytania o kod OTT, wyświetla się pytanie o PIN

Jeśli aplikacja do podpisu dokumentów prawidłowo obsługuje podpis mSzafir, to od razu powinno pojawić się okno z pytaniem o **kod OTT**, który jest niezbędny do autoryzacji podpisu.

Część aplikacji może błędnie rozpoznawać obsługę certyfikatów mSzafir. Jeśli pojawia się pytanie o **kod PIN**, obejściem może być podanie w tym polu dowolnego kodu PIN, np.: 1111.

Po zatwierdzeniu powinno się pojawić okno z pytaniem o **kod OTT**, gdzie należy wprowadzić kod z **aplikacji mobilnej mSzafir**. W dalszym kroku autoryzację operacji podpisu zatwierdź w aplikacji mobilnej.

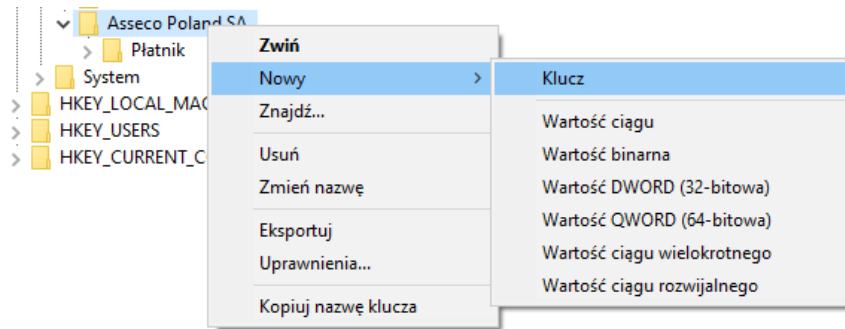
W przypadku dalszych problemów należy skontaktować się z dostawcą aplikacji do podpisu.

## 7. Podpis w programie Płatnik

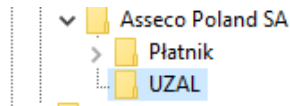
W przypadku oprogramowania Płatnik, aby możliwe było podpisanie danych z użyciem certyfikatu długoterminowego mSzafir, należy oprócz wskazania tego certyfikatu do podpisu, ustawić dodatkowo w rejestrze systemowym klucz **ZablokujTrybCichy** na wartość **1**.

W tym celu należy:

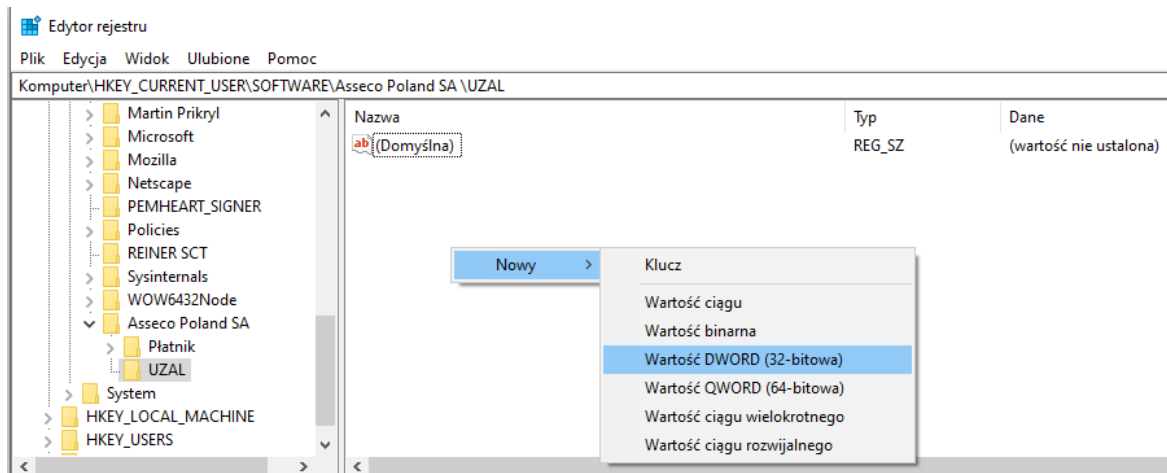
- 1) uruchomić **Edytor rejestru** (w polu wyszukiwania na pasku zadań wpisz słowo **regedit** lub kliknij prawym przyciskiem myszy przycisk Start i wprowadź **regedit**),
- 2) po uruchomieniu **Edytora rejestru** użytkownik może zostać poproszony o podanie danych jak login i hasło. Należy podać login i hasło użytkownika do systemu Windows.  
**WAŻNE!** Należy logować się w kontekście użytkownika systemu Windows, który korzysta z Płatnika a nie administratora systemu. W przypadku, gdy zmiana jest wprowadzana przez administratora należy przejść do punktu 8.
- 3) będąc na węźle „**HKEY\_CURRENT\_USER\SOFTWARE\Asseco Poland SA**” wybierz z menu Nowy -> Klucz



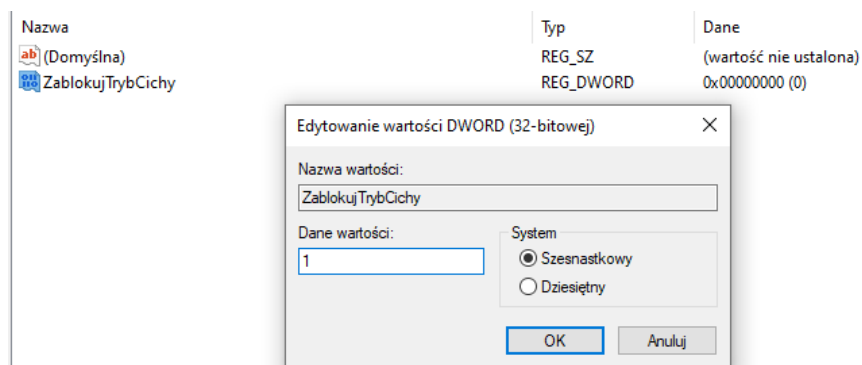
4) wybierz **UZAL**



5) wybierz **Nowy** -> **Wartość DWORD** i nadaj nazwę **ZablokujTrybCichy**

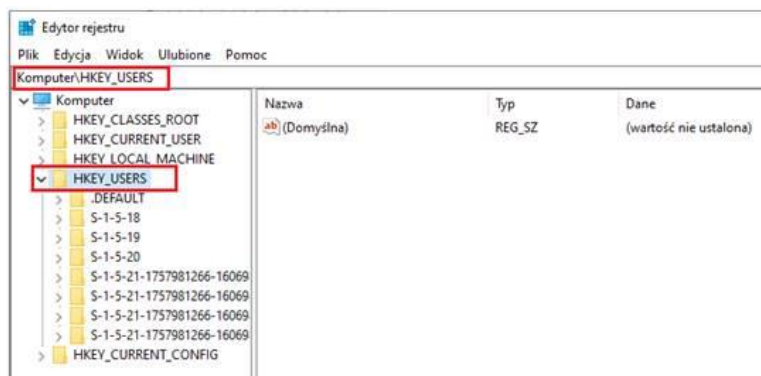


6) wybierz **Modyfikuj** i ustawiamy wartość **1**

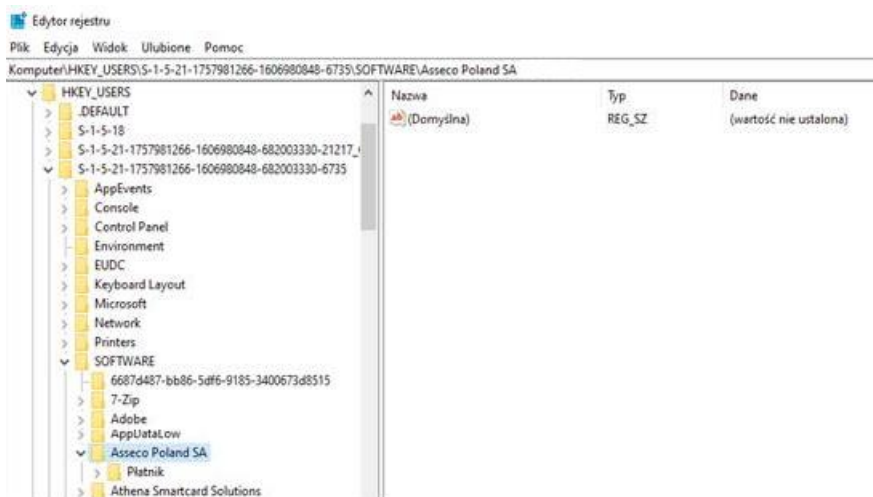


7) po wprowadzeniu zmian wykonaj jest restart komputera.

- 8) Jeśli zmiana jest wprowadzana przez administratora systemu to należy ją wprowadzić w odpowiednim profilu użytkownika systemu Windows, który korzysta z Płatnia. Profile użytkowników znajdują się w rejestrze systemowym w ramach **HKEY\_USERS**.



Po odnalezieniu odpowiedniego profilu, który zawiera w drzewie **SOFTWARE\Asseco Poland SA\Płatnik** należy postępować zgodnie z punktami 3 – 7.



Od tego momentu program Płatnik będzie mógł wykorzystać certyfikat mSzafor do podpisu.

### WAŻNE!

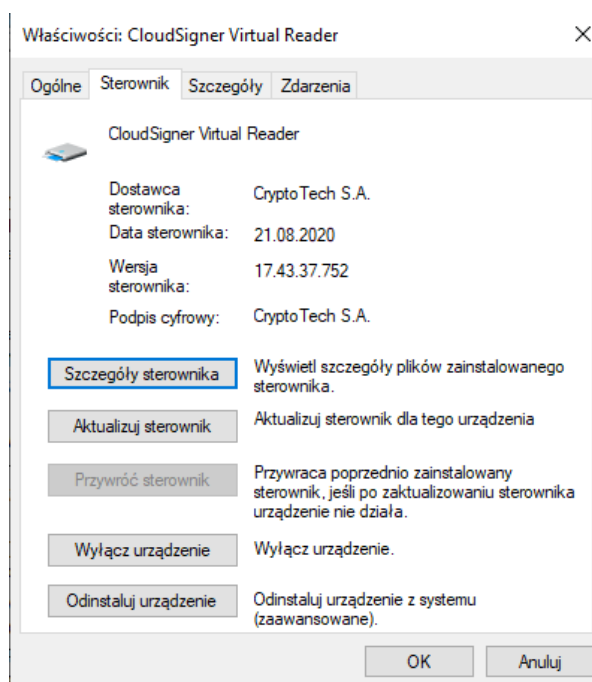
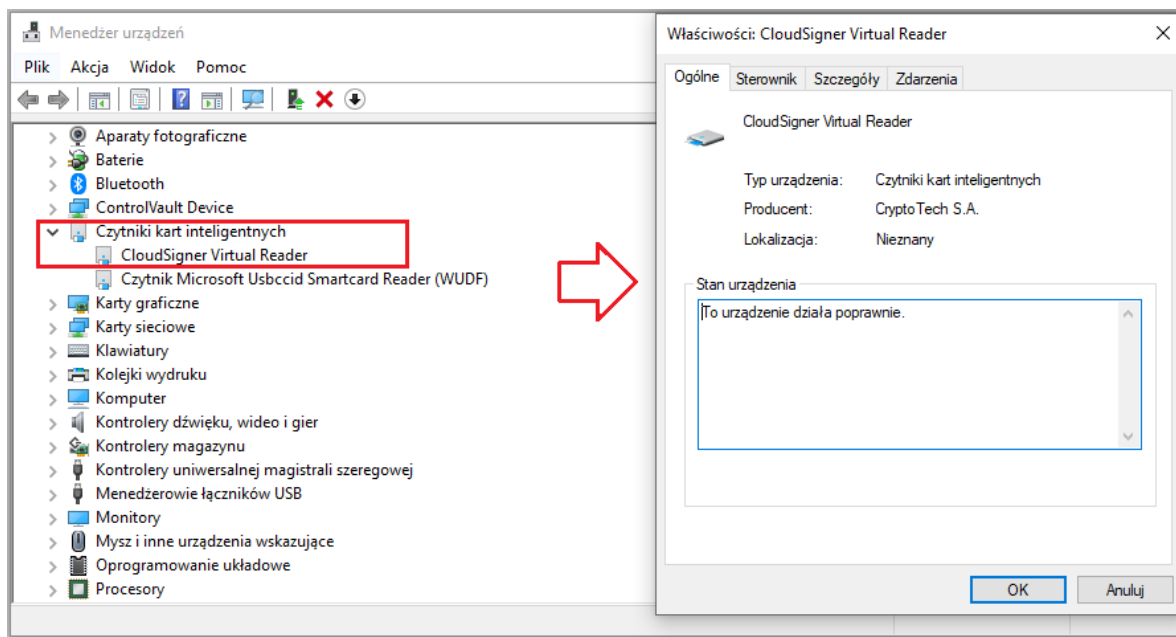
W przypadku Płatnika standardowe pytanie o PIN będzie się zawsze pojawiało - obejściem jest podanie w tym polu dowolnego PIN np.: 1111. Po zatwierdzeniu pojawi się okno z pytaniem o kod OTT, gdzie należy wprowadzić kod z aplikacji mobilnej mSzafor.

## 8. Wirtualny czytnik kart

Po instalacji oprogramowania **CryptoCard CloudSigner** w systemie Windows jest instalowany wirtualny czytnik kart. W razie problemów wskazujących na czytnik, zweryfikuj poprawność instalacji czytnika w **Menedżerze urządzeń**.

Poniżej znajduje się widok poprawnej instalacji:



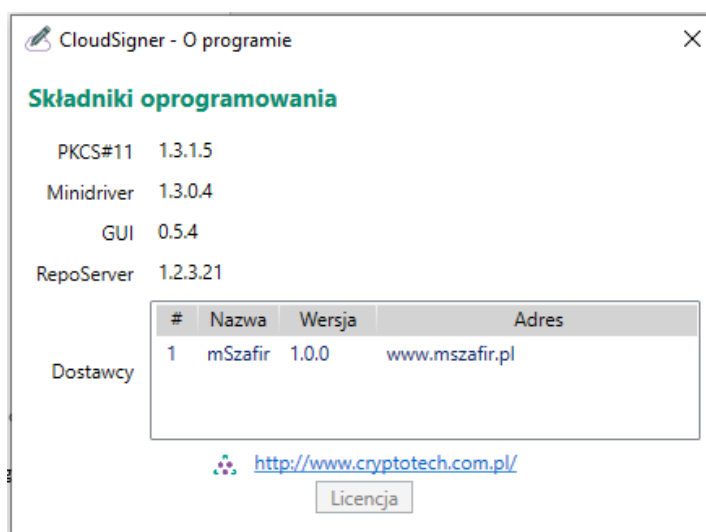


Jeżeli instalacja automatyczna nie powiodła się, można wykonać ją ręcznie poprzez wybranie opcji [Zainstaluj dla pliku CloudSignerMD.inf](#) znajdującej się w katalogu instalacyjnym:  
[C:\Program Files\CryptoTech\CryptoCard CloudSigner](#)

## 9. Zebranie logów diagnostycznych

W przypadku problemów z działaniem aplikacji lub podpisywaniem należy przekazać do KIR następujące informacje:

- logi, które znajdują się w katalogu domowym użytkownika w pliku [repo.log](#):  
`C:\Users\nazwa_uzytkownika\AppData\Local\CryptoTech\CloudSigner\repo.log`
- informację o wersji **CryptoCard CloudSigner** – należy najechać kursorem myszy na ikonę **CloudSigner** i wybrać opcję **O programie** z menu kontekstowego:



W przypadku pojawienia się problemów prosimy o kontakt:

e-mail: [kontakt.szafir@kir.pl](mailto:kontakt.szafir@kir.pl)