

Instrukcja dodania karty wirtualnej mSzafir w oprogramowaniu CloudSigner na potrzeby użycia certyfikatów mSzafir z poziomu aplikacji pracujących w systemie Windows

Aby dodać kartę wirtualną mSzafir, wykonaj następujące kroki:


1. Zainstaluj oprogramowanie **CryptoCard CloudSigner** od firmy CryptoTech udostępnione pod adresem:

https://www.elektronicznypodpis.pl/storage/file/core_files/2023/9/7/e3f68520d4c6e9b32bc0c40ca33730c6/cryptocardcloudsigner.exe

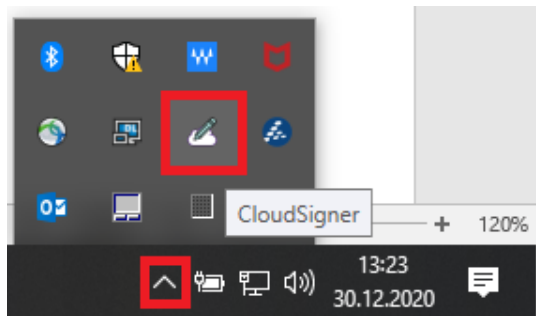
Ważne!

Aplikacja **CryptoCard CloudSigner** do prawidłowego działania wymaga:

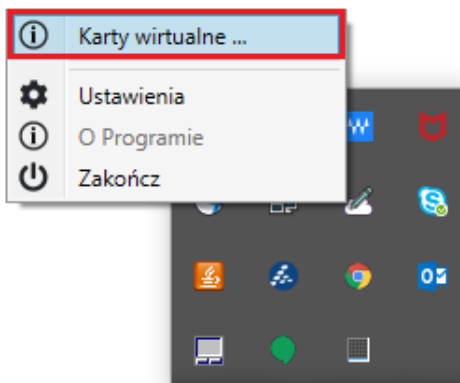
- oprogramowania **.NET Desktop Runtime x86**. Jeśli na stacji roboczej nie będzie stosownej wersji, wówczas automatycznie uruchomi się proces doinstalowania wymaganego oprogramowania. CloudSigner 1.8.1.96 lub nowszy wymaga **.NET Desktop Runtime x86** w wersji **6.0.11** lub nowszej (<https://dotnet.microsoft.com/en-us/download/dotnet/6.0>)
- dostępu do Internetu

Po instalacji aplikacja **CryptoCard CloudSigner**  będzie widoczna na rozwijanej liście działających aplikacji Windows. Jeżeli ikona aplikacji nie będzie dostępna na liście, wówczas wyszukaj

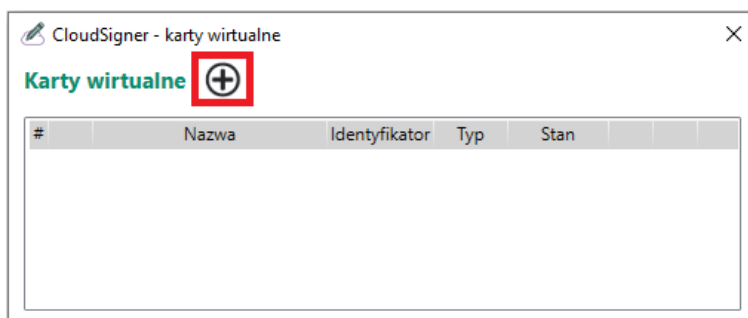
w menu Windows aplikację **CloudSignerUI** i uruchom ją. Ikona aplikacji  powinna być widoczna:



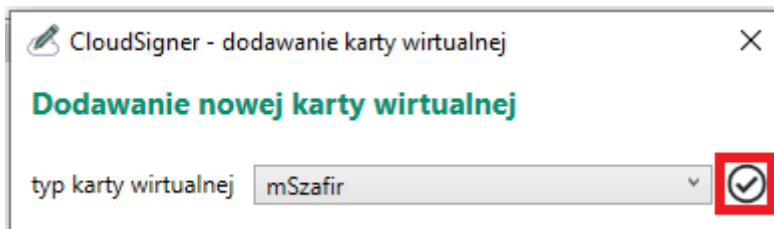
2. Najedź kursorem myszy na ikonę **CloudSigner** i wybierz opcję **Karty wirtualne** z menu kontekstowego:



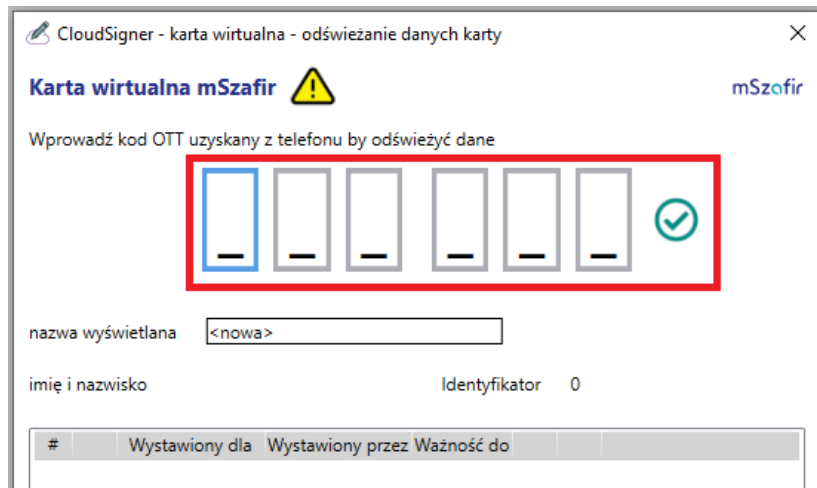
3. Kliknij przycisk **+** w oknie **Cloudsigner – karty wirtualne**:



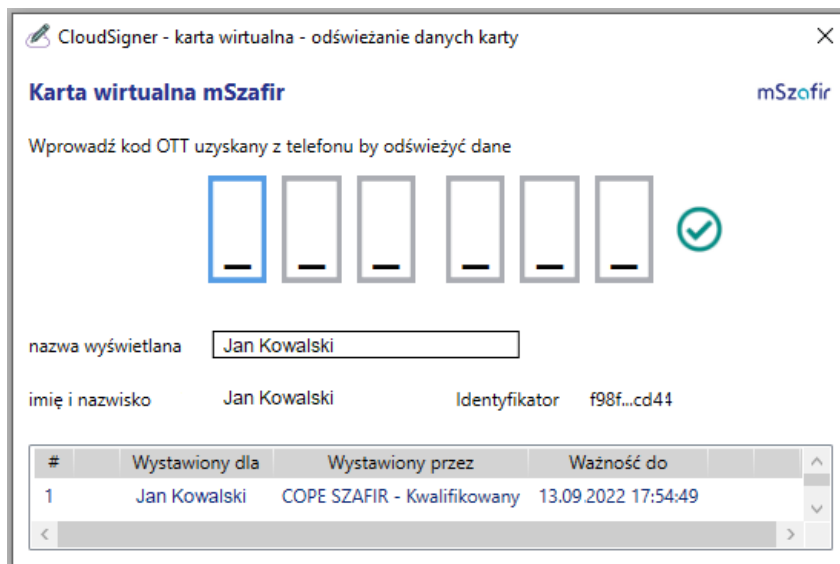
4. Wskaż typ karty wirtualnej **mSzafir** i kliknij **✓** :



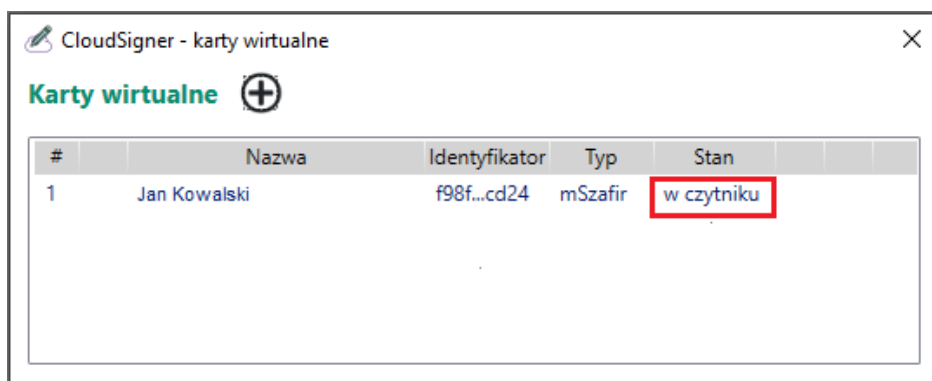
5. Uruchom aplikację mobilną **mSzafir** w swoim telefonie i wybierz opcję **Generuj kod**.
6. Kod wygenerowany w **aplikacji mobilnej mSzafir** wprowadź w polach przewidzianych na **kod OTT** i zatwierdź, klikając **✓** :



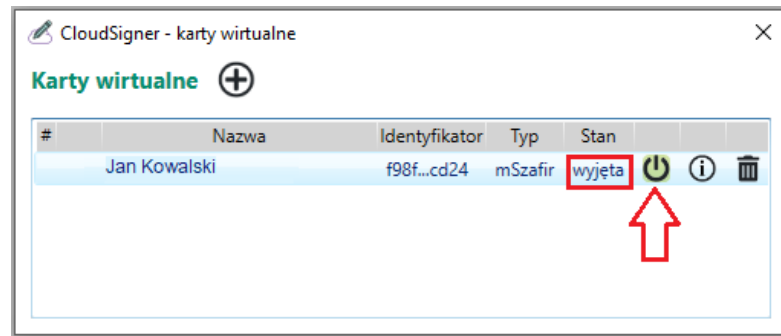
7. W aplikacji mobilnej mSzafir potwierdź autoryzację operacji.
8. Po autoryzacji w aplikacji CloudSigner zostanie zaprezentowana lista aktywnych certyfikatów mSzafir. Wszystkie widoczne na wirtualnej karcie certyfikaty zostały jednocześnie automatycznie zarejestrowane w systemie Windows. Zamknij okno i przejdź do widoku CloudSigner - Karty wirtualne, aby sprawdzić status karty:



9. Stan karty wirtualnej automatycznie otrzymuje status „w czytniku” i od tego momentu można już podpisywać dokumenty z użyciem certyfikatu mSzafir w wybranych aplikacjach.



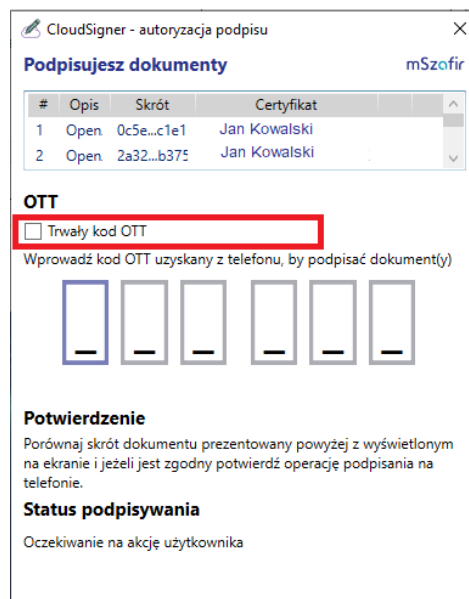
Jeśli karta ma stan „wyjęta”, najedź kursorem myszy na rekord z danymi karty i kliknij :



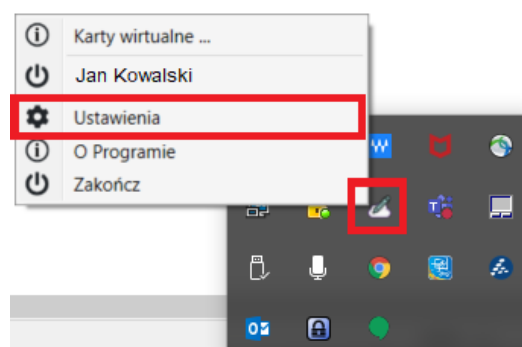
Stan karty wirtualnej powinien zmienić się na: „w czytniku”.

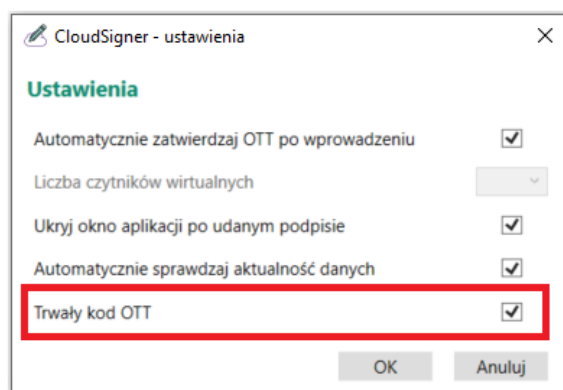
10. Jeżeli zamierzasz podpisywać duże ilości dokumentów włącz opcję Trwały kod OTT na etapie podpisu lub w ustawieniach CloudSigner, dzięki czemu nie będzie konieczności podawania kodu OTT przy każdym dokumencie. Będziesz proszony o potwierdzanie kolejnych podpisów w aplikacji mobilnej w czasie ważności kodu OTT. Po tym czasie będzie poproszony o podanie nowego kodu OTT. Minimalna wymagana wersja aplikacji CloudSigner wspierająca multipodpis to 1.6.2.89.

- a. Ustawienie opcji Trwały kod OTT na etapie podpisu



- a. Ustawienie opcji Trwały kod OTT na stałe w konfiguracji aplikacji





Ważne!

W przypadku użycia aplikacji Szafir rekomendowana jest wersja aplikacji Szafira 2.0 (build 657) lub nowsza.

11. Jeżeli aplikacje, z których korzystasz, wymagają wskazania biblioteki do obsługi karty, to 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

W przypadku pojawienia się problemów prosimy o kontakt:

Infolinia: (22) 545 55 55, e-mail: kontakt.szafir@kir.pl