

Ministerstwo Finansów Właściciel

# Instrukcja postępowania w celu uzyskania certyfikatu celnego oraz wykonania podpisu elektronicznego

nazwa dokumentu



nazwa Projektu

2.14 Wersja

07.02.2023 r.



# Spis treści

SŁ	OWN	NIK STOSOWANYCH SKRÓTÓW I TERMINÓW	3
1.	к	ONFIGURACJA KOMPUTERA	4
	1.1	INSTALACJA CERTYFIKATÓW CCK MF	4
	1.2	Konfiguracja zapory systemu Windows (Windows Firewall)	4
	1.3	Konfiguracja przeglądarki Mozilla Firefox	4
	1.4	KONFIGURACJA W MACUS	6
2.	II	NSTALACJA APLIKACJI CERTSIGN	9
	2.1	POBRANIE I URUCHOMIENIE INSTALATORA	9
	2.2	STATUS POŁĄCZENIA	9
	2.2	AUTOMATYCZNA INSTALACJA CERTYFIKATOW CCK MF	10
3.	C	D APLIKACJI CERTSIGN	11
	3.1	FUNKCJE I USTAWIENIA APLIKACJI CERTSIGN	11
4.	G	GENEROWANIE CERTYFIKATU	14
	4.1.	GENEROWANIE CERTYFIKATU DO MAGAZYNU SYSTEMU WINDOWS (CSP)	15
	4.2.	GENEROWANIE CERTYFIKATU PRZY WYKORZYSTANIU PKCS#11	17
	4.3.	GENEROWANIE CERTYFIKATU PRZY WYKORZYSTANIU KEYSTORE	
5.	v	WYKONANIE PODPISU ELEKTRONICZNEGO	21
	5.1	Wykonanie podpisu elektronicznego na PUESC	22
	5.2	Wykonanie podpisu z certyfikatem w magazynie Windows (CSP)	23
	5.3	WYKONANIE PODPISU Z KARTY KRYPTOGRAFICZNEJ ZGODNEJ Z PKCS#11	25
	5.4	Wykonanie podpisu z certyfikatem (kluczem) zapisanym w pliku <i>Keystore</i>	25
	5.5	WYKONANIE PODPISU ELEKTRONICZNEGO LOKALNIE NA KOMPUTERZE – W TRYBIE OFFLINE	26
6.	Z	GŁASZANIE PROBLEMÓW, PRZEGLĄDANIE LOGÓW	27
	6.1	DANE POTRZEBNE DO ANALIZY PROBLEMÓW Z DZIAŁANIEM APLIKACJI	27
	6.2	WŁĄCZANIE LOGOWANIA W APLIKACJI CERTSIGN	27
7.	Р	OBRANIE CERTYFIKATU LUB DOKUMENTU POTWIERDZENIA Z KONTA NA PUESC	28
8.	A	AKTUALIZACJA APLIKACJI CERTSIGN	29
9.	D	DODATEK A	30
	A.1 I	Manualna instalacja certyfikatów w systemie Windows	
	A.2 \	WERYFIKACJA POPRAWNOŚCI CERTYFIKATU OSOBISTEGO W SYSTEMIE WINDOWS	32
	A.3 I	Eksport certyfikatu z magazynu certyfikatów systemu Windows	33
	A.4 I	Import certyfikatu do magazynu certyfikatów systemu Windows (CSP)	
	A.5 (	Opis opcji Konfiguracja usług kryptograficznych	
	A.61	KOZWIĄZANIE PROBLEMOW Z POŁĄCZENIEM STRONY PUESC Z APLIKACJĄ CERTSIGN	40
_	A.7		
D	JUAT	IEK В	41
	B.1 F	PODPISANIE DANYMI Z WARSTWY ELEKTRONICZNEJ DOWODU OSOBISTEGO	41
	B.2 F	HUNKCJE SKALOWANIA ELEMENTOW INTERFEJSU GRAFICZNEGO	
	ы.3( для	UBSEUGA APLIKAUJI PRZEZ CZY I NIK EKRANU Najwigowanie i stepowanie ki awijatuda	43 12
	B.51	WSPÓŁ PRACA Z LISŁUGA MOBII NEGO PODPISU ELEKTRONICZNEGO	
B.5 WSPOŁPRACA Z USŁUGĄ MOBILNEGO PODPISU ELEKTRONICZNEGO B.6 Szczególne przypadki dotyczące kart z certyfikatami kwalifikov		Szczególne przypadki dotyczące kart z certyfikatami kwalifikowanymi	

	CDVM	Ministerstwo Finansów – PL	JESC.P4.4 – Program PUESC
PIUESC			
Wersja dokumentu	2.14	Data opracowania	2023-02-07

## Słownik stosowanych skrótów i terminów

Skrót / termin	Wyjaśnienie
Certyfikat celny	W rozumieniu niniejszej instrukcji jest to elektroniczne zaświadczenie wydane przez Centrum Certyfikacji Ministerstwa Finansów, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny zarejestrowanej na PUESC i które umożliwiają identyfikację tej osoby.
ID SISC	Unikalny numer identyfikacyjny nadawany osobom podczas procesu rejestracji w SISC.
Instrukcja e-Klient	Instrukcja elektronicznej rejestracji dla potrzeb zarządzania użytkownikami korzystającymi z usług SISC.
PUESC	Platforma Usług Elektronicznych Skarbowo-Celnych.
Regulamin	Regulamin dla certyfikatów cyfrowych emitowanych przez Centrum Certyfikacji Ministerstwa Finansów.
SC	Służba Celno-Skarbowa
SISC	System Informacyjny Skarbowo-Celny



## 1. Konfiguracja komputera

## 1.1 Instalacja certyfikatów CCK MF

Dla prawidłowej obsługi procesów generowania certyfikatów oraz wykonania podpisu konieczne jest pobranie i zainstalowanie certyfikatów Centrum Certyfikacji Ministerstwa Finansów (CCK MF). Aplikacja CertSign instaluje przy pierwszym uruchomieniu niezbędne certyfikaty w systemie Windows (dostępne są one przeglądarkom Internet Explorer, Edge, Chrome oraz Firefox – po uprzedniej konfiguracji. Opis konfiguracji Firefox znajduje się w rozdziale 1.3. W przypadku konieczności manualnej instalacji certyfikatów, dostępne są one na stronie *https://puesc.gov.pl/uslugi/uzyskaj-lub-uniewaznij-certyfikat-celny*, w menu *Elektroniczne podpisywanie dokumentów > Uzyskaj lub unieważnij certyfikat celny*, albo w *Moje dane > Certyfikaty celne*. Opis instalacji certyfikatów znajduje się w dodatku A.1

## 1.2 Konfiguracja zapory systemu Windows (Windows Firewall)

Aplikacja CertSign realizuje wewnątrz komputera połączenie ze stroną internetową. Konieczne może być manualne zezwolenie na komunikację pomiędzy przeglądarką i aplikacją, np. poprzez Windows Firewall. Może pojawić się ostrzeżenie, np. wyświetlane przez zaporę systemu Windows. Należy zaznaczyć wszystkie opcje zezwalające aplikacji CertSign na łączenie w sieciach i kliknąć na przycisk "Zezwalaj na dostęp". W przypadku stosowania oprogramowania antywirusowego z włączoną funkcją zapory (firewall), analizy ruchu, itp., należy w oprogramowaniu antywirusowym umożliwić:

- uruchomienie aplikacji CertSign
- odblokować komunikację pomiędzy przeglądarką a adresem localhost, porty 22443 oraz 22311.

## 1.3 Konfiguracja przeglądarki Mozilla Firefox

Przeglądarka Firefox posiada własny *Menedżer certyfikatów*, w którym przechowywane są certyfikaty wymagane do poprawnej współpracy przeglądarki z aplikacją CertSign. Aby przeglądarka korzystała z certyfikatów zarejestrowanych w magazynie certyfikatów systemu Windows, należy:

W pasku adresu wpisać about:config (i zatwierdzić).



Potwierdzić komunikat ostrzeżenia i wybrać Akceptuję ryzyko, kontynuuj

Zachowaj ostrożność
Modyfikacja zaawansowanych preferencji może wpłynąć na wydajność lub bezpieczeństwo programu Firefox.
✓ Wyświetlanie tego ostrzeżenia za każdym razem
Akceptuję ryzyko, kontynuuj

5

Wyszukać parametr *security.enterprise\_roots.enabled* oraz ustawić jego wartość na *true* (wartość logiczna, zmiana strzałkami po prawej stronie).

security.enterprise\_roots.enabled true  $\rightleftharpoons$   $\backsim$ 

Zamknąć przeglądarkę.

Po ponownym uruchomieniu przeglądarka powinna być gotowa do korzystania z certyfikatów zarejestrowanych w magazynie certyfikatów Windows. W przypadku, gdyby to ustawienie nie działało, można manualnie zarejestrować certyfikaty CCK MF w *Menadżerze certyfikatów* Firefox.



Ze strony https://puesc.gov.pl/uslugi/uzyskaj-lub-uniewaznij-certyfikat-celny pobrać i zapisać na dysku certyfikaty CCK MF Root, CCK MF Infrastruktura i Aplikacje, CCK MF Wewnetrzne, CCK MF Zewnetrzne.

LISTA CERTYFIKATÓW CELNYCH Lista nie zawiera certyfikatów kwalifikowanych oraz kluczy do bezpiecznej transmisji danych wydanych przez CBTD i IC Kraków							
NUMER SERYJNY:	WAŻNY OD:	WAŻNY DO:	AKCJE:				
Generuj certyfikat celny							
TCK ME Infractruktura i Anlikacia	ert						
CCK_MF_Infrastruktura_i_Aplikacje. CCK_MF_Root.crt	crt						
ICK_MF_Infrastruktura_I_Aplikacje. ICK_MF_Root.crt ICK_MF_Wewnetrzne.crt	crt						

W przeglądarce wejść w menu Ustawienia albo w pasku wpisać about:preferences i zatwierdzić.

$\leftarrow$ ·	$\rightarrow$	С	单 Firefox	about:preferences	☆
W usta	awie	eniach prze	iść do Pryv	vatność i bezpieczeństwo oraz wybrać Wyświetl certyfikaty.	



W *Menedżerze certyfikatów* wskazać *Organy certyfikacji*, wybrać *Importuj*, wskazać kolejno certyfikaty z dysku i zatwierdzić import.

Menedžer certyfikatów									
Użytkownik	Decyzje uwierzytelniania	Osoby	Serwery	Organy o	certyfikacji				
/lasz certyfikaty, l	które identyfikują następujące o	rgany certyfik	cacji:						
Nazwa certyfika	tu	Urząd	zenie zabezp	ieczające		E.			
✓ AC Camerfirm	a S.A.					^			
Chambers of	of Commerce Root - 2008	Builtin (	Builtin Object Token						
Global Cha	mbersign Root - 2008	Builtin (	Builtin Object Token						
✓ AC Camerfirm	a SA CIF A82743287								
Camerfirma	Chambers of Commerce Root	Builtin (	Object Token						
Camerfirma	a Global Chambersign Root	Builtin (	Object Token			~			
Wyświetl	E <u>d</u> ytuj ustawienia zaufania	. l <u>m</u> po	rtuj	<u>E</u> ksportuj	<u>U</u> suń lub przest	ań ufać			
						ок			

Podczas zatwierdzania zweryfikować dane certyfikatu i ustawić zasady zaufania.



Pobieranie certyfikatu	X
Otrzymano prośbę o dołączenie nowego organu certyfikacji do listy zaufanych organów.	
Czy zakwalifikować "Centrum Certyfikacji Ministerstwa Finansow" jako źródło godne zaufania w następujących przypadkach?	
🔽 Zaufaj temu CA przy identyfikacji witryn internetowych.	
Zaufaj temu CA przy identyfikacji użytkowników poczty.	
Jeżeli jest to możliwe, przed udzieleniem zgody należy zapoznać się z certyfikatem tego organu or jego polityką i stosowanymi procedurami.	az
Wyświetl Sprawdź certyfikat CA	
OK Anuluj	

Opcja Wyświetl pozwala zweryfikować dane certyfikatu.

Nazwa wystawcy	
Państwo	PL
Organizacja	Ministerstwo Finansow
Jednostka organizacyjna	Krajowa Administracja Skarbowa
Nazwa pospolita	Centrum Certyfikacji Ministerstwa Finansow
Ważność	
Nieważny przed	Wed, 10 May 2017 06:17:03 GMT
Nieważny po	Fri, 04 May 2040 06:17:03 GMT
Informacje o <mark>klucz</mark> u	
publicznym	
Algorytm	RSA
Rozmiar klucza	4096
Wykładnik	65537
Modulo	E8:97:6F:2C:EA:BE:8A:72:9F:46:AA:1C:A9:7E:D1:AD:30:8F:C5:D0:DF:8C:FB:DF:DD:
Różne	
Numer serviny	15
··· 21 ···	enters companies and

Operacje importu należy powtórzyć dla wszystkich certyfikatów CCK MF.

## 1.4 Konfiguracja w macOS

Należy zaimportować do Pęku kluczy certyfikaty centrów certyfikacji MF.

🗯 Finder Plik Ed	rcja Widok Idź Okno Pomoc 🔒	*	((;	۰ I	≜	<b>(</b> )	Pt. 11:54	admin	Q	5	Ξ
	🔯 Przeszukiwanie "Ten Mac"							-	2.		
$\langle \rangle$				Q	oęk kl	uczy	<				8
Ulubione	Szukaj: Ten Mac "Narzędzia"			Na	zwy pli	ków		-			
Wszystkie moje pliki	Dzisiaj			P	asując	e nazv	vy: pęk kluc:	zy			
iCloud Drive											
() AirDrop 1.	3.										
A: Programy											
Biurko	Dostęp do pęku										
Dokumenty	kluczy										

W Dostęp do pęku kluczy należy wybrać Plik > Importuj rzeczy ...





Zostanie otwarte okno umożliwiające wskazanie położenia plików z certyfikatami centrów certyfikacji.

🗯 🛛 Dostęp do pęku klu	czy Plik Edycja Widok	Okno Pomoc	
Kliknij, aby zablokować pęk	kluczy login.		Dostęp do pęku kluczy
Pęki kluczy			் ரீட் ெ Szukai
💣 login			
<ul> <li>Usługi katalogowe</li> <li>iCloud</li> <li>System</li> </ul>	Ulubione Ulubione Wszystkie moje pliki Ciloud Drive	Certificar	Completion Control Control
Systemotynkaty growne	Programy	localhost.crt	test cck mf TEST CCK MF
Kategoria     Wszystkie rzeczy     L. Hasła     Bezpieczne notatki     Moje certyfikaty	<ul> <li>Biurko</li> <li>Dokumenty</li> <li>Pobrane rzeczy</li> </ul>	Certificar	
% Klucze Certyfikaty	Urządzenia Płyta zdalna	TEST CCK MF Zewnetrzne.crt	test cck mf.crt
	Oncie		Anului Otwórz

Należy wskazać plik z certyfikatem (1) i kliknąć *Otwórz* (2). Certyfikat zostanie zaimportowany i uzyska status "niewiarygodny".



Należy kliknąć na certyfikat i rozwinąć Opcje zaufania.



• •	TEST CCK MF
Centifecte Główny urząd certyfika Wygasa: niedziela, 11 r • Ten certyfika główn	acji narca 2040 13:40:35 Czas środkowoeuropejski standardowy y nie jest wiarygodny
Używając tego certyfi	katu: Użyj domyślnych systemowych ᅌ ?
SSL (Secure Sockets L	ayer) 🛛 brak wskazanej wartości 💦 😋
Bezpieczna poczta (S/M	IME) brak wskazanej wartości 🔷
Rozszerzone uwierzytelnienie (	EAP) brak wskazanej wartości ᅌ
Ochrona IP (IF	Isec) brak wskazanej wartości
Podpisywanie	kodu brak wskazanej wartości
Znakowanie cza	isem brak wskazanej wartości
Zacady podetawowe Y	509 brak wskazanej wartości
Lasady polatawowe A	
▼ Szczegóły	
Nazwa podmiotu	
Kraj	PL
Organizacja	Ministerstwo Finansow
Jednostka organizacyjna	Krajowa Administracja Skarbowa
Powszechna nazwa	TEST CCK MF
Nazwa wystawcy	
Kraj	PL
Organizacja	Ministerstwo Finansow
Jednostka organizacyjna	Krajowa Administracja Skarbowa
Powszechna nazwa	TEST CCK MF
Numer cerviny	0
Wersia	3
Algorytm podpisu	- SHA-512 z szyfrowaniem RSA ( 1.2.840.113549.1.1.13 )
Parametry	brak
Nieważny przed	piątek, 17 marca 2017 13:40:35 Czas środkowoeuropejski standardowy
Nieważny po	niedziela, 11 marca 2040 13:40:35 Czas srodkowoeuropejski standardowy

W *Opcje zaufania* należy w polu *Używając tego certyfikatu* ustawić *Zawsze ufaj* i zapisać wprowadzone ustawienia.

•••		TEST C	CCK MF
Certificate	TEST CCK MF Główny urząd certyfikacji Wygasa: niedziela, 11 marca Ten certyfikat główny nie j	2040 13:40:35 Czas est wiarygodny	środkowoeuropejski standardowy
Opcje za	ufania		· /
	Używając tego certyfikatu:	Zawsze ufaj	
5	SSL (Secure Sockets Layer)	Zawsze ufaj	-
B	ezpieczna poczta (S/MIME)	Zawsze ufaj	٥
Rozszerz	one uwierzytelnienie (EAP)	Zawsze ufaj	٥
	Ochrona IP (IPsec)	Zawsze ufaj	٥
	Podpisywanie kodu	Zawsze ufaj	٥
	Znakowanie czasem	Zawsze ufaj	٥
	Zasady podstawowe X.509	Zawsze ufaj	٥

Operacje należy powtórzyć dla wszystkich certyfikatów CCK MF.



## 2. Instalacja aplikacji CertSign

## 2.1 Pobranie i uruchomienie instalatora

Pliki instalacyjne aplikacji CertSign dostępne są na portalu PUESC w menu *Elektroniczne podpisywanie dokumentów > Dowiedz się więcej o systemie PKI* 

https://puesc.gov.pl/uslugi/elektroniczne-podpisywanie-dokumentow

Udostępnionych jest kilka wersji programu, spośród których należy wybrać wersję odpowiednią dla używanego systemu operacyjnego komputera. Po pobraniu należy uruchomić instalator aplikacji.

# W systemach Microsoft Windows aplikacja instaluje się w profilu użytkownika, bez konieczności podnoszenia uprawnień do poziomu lokalnego administratora.

Aplikacje nie są przewidziane do używania na serwerowych wersjach systemów operacyjnych, ani do pracy terminalowej.

## 2.2 Status połączenia

Aplikacja wskazuje dwa możliwe statusy połączenia ze stroną internetową:

🎋 CertSign	🍄 CertSign		
Krajowa Administracja Status połączenia: połączony Skarbowa	Krajowa Administracja Status połączenia: brak połączenia		
🚾 Certyfikaty/Log 💋 Podpis	🛅 Certyfikaty/Log 🙎 Podpis		

## Bezpośrednio po uruchomieniu aplikacja wskazuje *Status połączenia:* brak połączenia, i jest to sytuacja prawidłowa.

Komunikat *Status połączenia:* **połączony** informuje, że strona PUESC prawidłowo nawiązała połączenie z aplikacją CertSign. Status **połączony** jest wymagany przy generowaniu certyfikatu oraz przy podpisywaniu dokumentu na PUESC. W przypadku podpisywania pliku z dysku komputera nie jest wymagane połączenie ze stroną PUESC. Status **brak połączenia** nie jest w takim przypadku objawem nieprawidłowego działania.

Aplikacja po ręcznym uruchomieniu będzie sygnalizowała status **brak połączenia** do czasu uruchomienia na stronie PUESC operacji podpisywania dokumentu lub generowania certyfikatu celnego.

W przypadku braku połączenia podczas generowania certyfikatu lub podpisywania dokumentu na PUESC (*Status połączenia:* brak połączenia) należy skonfigurować komputer oraz przeglądarkę internetową zgodnie z opisami w rozdziale 1. W trybie brak połączenia możliwe jest podpisywanie plików z dysku na komputerze (offline), o ile użytkownik posiada certyfikat.

W systemach z rodziny Linux oraz Mac OS X rekomendowane jest używanie przeglądarki Firefox, po uprzednim skonfigurowaniu.

W przypadku występowania problemów z połączeniem należy postępować zgodnie z opisem znajdującym się w dodatku A.6



## 2.2 Automatyczna instalacja certyfikatów CCK MF

W systemach Microsoft Windows aplikacja przy pierwszym uruchomieniu sprawdza, czy zainstalowane są certyfikaty Centrum Certyfikacji Ministerstwa Finansow. W przypadku ich braku aplikacja automatycznie proponuje instalację.

Ostrzeżer	ie o zabezpieczeniach	$\times$		
	Za chwilę zostanie zainstalowany certyfikat z urzędu certyfikacji, który rzekomo reprezentuje:			
	Centrum Certyfikacji Ministerstwa Finansow			
	System Windows nie może zweryfikować, czy certyfikat rzeczywiście pochodzi od "Centrum Certyfikacji Ministerstwa Finansow". Należy potwierdzić jego pochodzenie, kontaktując się z "Centrum Certyfikacji Ministerstwa Finansow". W procesie będzie pomocna następująca liczba:			
	Odcisk palca (sha1): 3135E42E 93CB89DC BB279703 A98B230A 4356092D			
	Ostrzeżenie: Jeśli ten certyfikat główny zostanie zainstalowany, system Windows będzie automatycznie ufać każdemu certyfikatowi wystawionemu przez ten urząd certyfikacji. Instalacja certyfikatu z niepotwierdzonym odciskiem palca to potencjalne zagrożenie.Kliknięcie przycisku Tak oznacza, że decydujesz się podjąć to ryzyko.			
	Czy chcesz zainstalować ten certyfikat?			
	Tak Nie			

Po poprawnej instalacji certyfikaty dostępne są dla przeglądarek: Internet Explorer, EDGE, Chrome (przeglądarki korzystające z Windows CSP) a także Firefox, po skonfigurowaniu zgodnie z opisem w rozdziale 1.3.



## 3. O aplikacji CertSign

Aplikacja CertSign realizuje dwie funkcje:

- 1. generowanie certyfikatów i obsługa kluczy kryptograficznych,
- 2. wykonanie podpisu elektronicznego w trybach online i offline.

Aplikacja współpracuje z przeglądarkami: Chrome, Firefox, Internet Explorer 11, Edge.

## 3.1 Funkcje i ustawienia aplikacji CertSign

**Status połączenia** – informuje czy aplikacja nawiązała połączenie ze stroną PUESC. Status połączenia przyjmuje następujące wartości: **połączono** lub **brak połączenia**. Podczas pracy w trybie offline brak połączenia jest stanem prawidłowym.

W trybie połączono (*online*) aplikacja wykonuje operacje w tle strony internetowej i po ewentualnym wybraniu opcji należy zminimalizować okno CertSign do paska zadań.



Klikając link "Pomoc" uzyskuje się dostęp do instrukcji działania aplikacji.

W zakładce "*Certyfikaty/Log"* prezentowany jest aktualny wybór certyfikatu służącego do wykonywania podpisu elektronicznego (przy pierwszym uruchomieniu okienko jest puste). Poniżej wyświetlany jest log aplikacji. Ustawienie poziomu logowania "*Pełny*" powinno być używane do gromadzenia informacji dla help-desku, w przypadku problemów z aplikacją.

Opcja *"Zmień certyfikat"* uruchamia dostęp do konfiguracji usług kryptograficznych, gdzie możliwy jest wybór nośnika kluczy/certyfikatów zgodnego z CSP, PKCS#11 lub Java™ Keystore. Możliwe jest także

![](_page_11_Picture_0.jpeg)

wskazanie położenia pliku sterownika (biblioteki \*.dll) standardu PKCS#11, lub pliku do przechowywania zaszyfrowanych kluczy na dysku (Keystore). Opis poszczególnych opcji dostępny jest w dodatku A.5.

Wyboru certyfikatu używanego w procesie składania podpisu elektronicznego dokonuje się przyciskiem *Zmień certyfikat*. W pierwszej kolejności zostanie wyświetlone okno konfiguracji usług kryptograficznych, gdzie dokonuje się wyboru magazynu przechowującego certyfikaty.

KONFIG	JURACJA			
alugi kryptogra	ficzne:			
CSP				
O PKCS #11	C:\Program Files	s\ENCARD\enig	map11-x64.dll	
				Wybierz
○ Keystore				
			Utwórz	Wybierz

Po wybraniu żądanej usługi i zatwierdzeniu przyciskiem *OK*, wyświetlone zostanie okno wyboru certyfikatu ze wskazanego magazynu certyfikatów.

Wystawiony dla:	Wydany przez:	Termin ważności:	Numer seryjny:	
	CCK MF Zewnetrzne	26/05/2022 08:11:14	1ca35	
	TEST CCK MF Zewnetrzne	26/05/2022 10:24:15	235b	
, i	TEST CCK MF Zewnetrzne	22/06/2023 09:00:05	2634	
i i i i i i i i i i i i i i i i i i i	TEST CCK MF Zewnetrzne	26/05/2022 10:28:35	235e	
czegóły certyfikatu				
lumer seryjny :				23

Wyboru certyfikatu dokonuje się z listy, zaznaczając certyfikat (zostanie on podświetlony kolorem) i klikając przycisk *OK*.

W zakładce "*Podpis*" dostępne są funkcje do lokalnego wykonania podpisu elektronicznego na pliku pobranym z dysku komputera. Do wykonania podpisu nie jest potrzebne uruchamianie PUESC ani nawiązywanie połączenia. Szczegóły opisane są w rozdziale 5.

Zaznaczenie opcji **"Sugeruj format podpisu"** powoduje automatyczne wybranie formatu i typu podpisu, na podstawie typu pliku wybranego do podpisania. Domyślnie opcja jest włączona. Jej odznaczenie powoduje odblokowanie możliwości ręcznego ustawiania parametrów podpisu.

![](_page_12_Picture_0.jpeg)

Parametry podpisu	
Format podpisu	
Algorytm skrótu	SHA256 ○ SHA512
Typ podpisu Poziom podpisu	Otaczający Otoczony Zewnętrzny
	🔽 Sugeruj format podpisu

Aplikacja umożliwia **skalowanie czcionek ekranowych** do trzech rozmiarów:

- Standardowy
- Większy
- Największy

Aby zmienić rozmiar czcionek, należy wybrać jeden z przycisków skalowania (A A A), który nie jest aktualnie wybrany. Każdy kolejny rozmiar jest większy od poprzedniego półtorakrotnie. Oznacza to, że powiększenie rozmiaru *standardowego* do *większego* skutkuje wzrostem aktualnego rozmiaru czcionek o 150%, zaś do *największego* – o 225%. Tak samo, zmniejszenie z *największego* do *większego* zmniejszy poziom z 225% rozmiaru *standardowego* do 150%, a powrót do *standardowego* pomniejszy aktualny do wartości domyślnej (100%). Skalowanie może nie działać na wyświetlaczach o niższych rozdzielczościach – aplikacja weryfikuje ten parametr w celu ochrony przed nadmiernym powiększaniem elementów.

![](_page_12_Picture_7.jpeg)

**Zmianę wersji językowej** na angielską wykonuje się klikając na pole PL. Przycisk "Zamknij" kończy działanie aplikacji.

Aplikacja posiada funkcję **"Autodiagnoza"**, która umożliwia sprawdzenie gotowości aplikacji do wykonywania podpisów. Aplikacja sprawdza dostępność portów sieciowych oraz wykonuje test podpisywania, używając certyfikatu wskazanego w zakładce *"Certyfikaty/Log"*. Aplikacja będzie żądać podania hasła zabezpieczającego klucz prywatny. Jeśli użytkownik nie posiada certyfikatu, test podpisu nie powiedzie się. Autodiagnoza zapisuje informacje o przebiegu testu w logu aplikacji i wyświetla okno raportu – Wynik autodiagnozy.

![](_page_13_Picture_0.jpeg)

## 4. Generowanie certyfikatu

Certyfikat celny może uzyskać wyłącznie osoba posiadająca aktywny ldSISC i zarejestrowana w tzw. procedurze pełnej. Niezarejestrowany użytkownik PUESC powinien, w pierwszej kolejności, dokonać rejestracji, wypełniając *Wniosek o rejestrację osoby fizycznej w SISC*.

PUESC udostępnia funkcjonalność generowania certyfikatu celnego. Do zarządzania oraz generowania certyfikatów celnych system posiada dedykowany widok, dostępny w *Moje dane > Certyfikaty celne*. W celu wygenerowania nowego certyfikatu należy wybrać opcję "Generuj certyfikat celny"

Certyfikaty Celne						
LISTA CERTYFIKATÓW CELNYCH Lista nie zawiera certyfikatów kwalifikowanych oraz kluczy do bezpiecznej transmisji danych wydanych przez CBTD i IC Kraków						
NUMER SERYJNY: WAŻNY OD: WAŻNY DO: AKCJE:						
Generuj certyfikat celny						
CCK_MF_Infrastruktura_i_Aplikacje.crt						

UWAGA: W celu wygenerowania kluczy kryptograficznych należy, przed wybraniem *Generuj certyfikat celny,* pobrać oraz zainstalować aplikację CertSign. Jeśli aplikacja nie będzie poprawnie zainstalowana, generowanie kluczy nie będzie możliwe.

Po wybraniu *Generuj certyfikat celny* system wyświetli komunikat z regulaminem usługi. Poniżej regulaminu, przed przejściem do kolejnego kroku, należy zaznaczyć oświadczenia, po czym przeprowadzić weryfikację captcha. Na koniec zatwierdzić akcję przyciskiem "**Potwierdź**".

<ul> <li>Zaznaczając poniższe pole Subskrybent akceptuje postan Treść zobowiązań i oświadczenie Subskrybenta zostaną u</li> <li>Wyrażam zgodę na przetwarzanie moich danych osi obowiązków podatkowych, obsługi i wsparcia przed monitorowaniu przewozu towarów na platformie el w art. 2 ust.1 pkt 5 ustawy z dnia 2 grudnia 2016 r. o Do wygenerowania certyfikatu celnego wymagany jesi k</li> </ul>	owienia Regulaminu. Zaznaczenie mieszczone na potwierdzeniu wy obowych w celu świadczenia usłu, obowych w celu uzyskania dostęp siębiorcy w prawidłowym wykony ektronicznej PUESC realizowanych o krajowej Administracji Skarbowe st program CertSign, aby pobrac i m not a robot	e poniższego pola oznacza złożenie oświ dania certyfikatu. Należy pobrać je i prze g przez Centrum Certyfikacji Ministerstw u do obsługi i wsparcia podatnika i płatr waniu obowiązków celnych oraz obowią n przez Krajową Administrację Skarbową ej. <b>ć i skonfigurować program przejdź do</b>	adczenia woli w tormie elektronicznej. achowywać w bezpiecznym miejscu. a Finansów. tika w prawidłowym wykonywaniu zków wynikających z ustawy o w interesie publicznym, określonym strony PKI-CertSign
✓ Potwierdź			Anuluj

Uwaga: po wybraniu *Potwierdź* może pojawić się komunikat z pytaniem, czy otworzyć aplikację CertSign. Jeśli aplikacja nie była uruchomiona należy zatwierdzić, zezwalając przeglądarce na otwarcie programu.

Open CertSign?				
http://172.25.45.64:9080 wants to open this application.				
	Open CertSign	Cancel		

![](_page_14_Picture_0.jpeg)

## 4.1. Generowanie certyfikatu do magazynu systemu Windows (CSP)

Po uruchomieniu aplikacji w trybie generowania certyfikatu zostanie wyświetlone okno konfiguracji usług kryptograficznych. Należy zaznaczyć opcję "*CSP*" i potwierdzić wybór przyciskiem "*OK*".

Konfiguracja usług kryptograficznych	>
	Q
Usługi kryptograficzne:	
• CSP	

Jeśli aplikacja do generowania certyfikatów nigdy nie była uruchamiana, opcja CSP jest domyślnie wybrana. W następnym kroku należy dokonać wyboru dostawcy usługi CSP służącej do generowania certyfikatu.

Dostępni dostawcy CSP:		
Microsoft Enhanced Cryptogra	aphic Provider v1.0	$\sim$
Krajowa Administracja Skarbowa	ОК	Anuluj

W przypadku generowania kluczy do **magazynu systemowego Windows**, należy wybrać z listy rozwijanej *Microsoft Enhanced Cryptographic Provider*... i zatwierdzić "*OK*".

Wyświetli się okno zabezpieczeń generowanego klucza. Należy w nim wybrać opcję Ustaw poziom zabezpieczeń ...

Tworzenie nov	rego klucza wymiany RSA 📃 🗮 🗮	
	Aplikacja tworzy element chroniony.	
	Klucz prywatny Crypto API	
	Ustawiono wysoki Ustaw poziom zabezpieczeń	] [
	OK Anuluj Szczegóły	

**Należy ustawić hasło składające się z co najmniej 12 znaków** (dużych i małych liter, cyfr oraz znaków specjalnych), a następnie zatwierdzić przyciskiem *Zakończ*.

![](_page_14_Figure_10.jpeg)

**Hasło jest poufne** i niezbędne do posługiwania się certyfikatem. Należy zabezpieczyć je w sposób uniemożliwiający dostęp innym osobom. **Hasła nie można odzyskać z PUESC** – jest ono tworzone i przechowywane lokalnie.

![](_page_15_Picture_0.jpeg)

W kolejnym oknie należy potwierdzić wybór ustawienia wysokiego poziomu zabezpieczeń przyciskiem OK.

Tworzenie no	vego klucza wymiany RSA
	Aplikacja tworzy element chroniony. Klucz prywatny CryptoAPI
	Ustawiono wysoki poziom zabezpieczeń
	OK Anuluj Szczegóły

Następuje generowanie kluczy kryptograficznych i certyfikatu. Proces ten jest niewizualny i może potrwać kilka minut. Po jego zakończeniu certyfikat jest automatycznie instalowany w komputerze użytkownika. Wygenerowany w ten sposób certyfikat jest eksportowalny, co oznacza, że możliwe jest przeniesienie go na inny komputer.

Po wygenerowaniu certyfikatu jego dane będą wyświetlone w oknie *Szczegóły certyfikatu...* aplikacji CertSign.

🖼 Wybrany certy	fikat do podpisu	
📷 Szczegóły ce	rtyfikatu	Zmień certyfikat
Wystawiony dla:	UID=PL431119218570000, O=PUESC, C=PL, CN= <b>CARA</b> , GIVENNAME= <b>CARA</b> , SURNAME= <b>CARA</b> , SURNAME= <b>CARA</b> , SURNAME= <b>CARA</b> , SURNAME	
Wystawione przez:	CN=TEST CCK MF Zewnetrzne, OU=Krajowa Administracja Skarbowa O=Ministerstwo Finansow, C=PL	
Ważny do:	25/08/2023 17:13:26	
Nr seryjny:	270a	

W kolejnym kroku należy ze strony PUESC pobrać dokument potwierdzający wydanie certyfikatu. Dokument pobiera się wybierając opcję *Pobierz potwierdzenie*.

![](_page_15_Picture_7.jpeg)

Dokument potwierdzający wydanie certyfikatu zalecamy wydrukować i przechowywać w bezpiecznym miejscu, ponieważ zawiera on kod pozwalający na zawieszenie lub unieważnienie certyfikatu za pośrednictwem help-desk.

Dokument potwierdzający wydanie certyfikatu oraz część publiczną certyfikatu (bez klucza prywatnego), można pobrać ponownie, zgodnie z opisem w rozdziale 7.

![](_page_16_Picture_0.jpeg)

## 4.2. Generowanie certyfikatu przy wykorzystaniu PKCS#11

Opcja ta wykorzystywana jest w przypadku certyfikatów zapisywanych na kartach kryptograficznych, niezależnie od posiadanego systemu operacyjnego. Jest to najbezpieczniejsza metoda przechowywania kluczy kryptograficznych i certyfikatu. Wykorzystując tę metodę, użytkownik musi posiadać zgodny ze standardem PKSC#11 sterownik karty kryptograficznej, dostarczony przez jej producenta. Klucze generowane są bezpośrednio na karcie kryptograficznej, co umożliwia użytkownikowi bezpieczne wykorzystanie na wielu komputerach.

Nie zalecamy generowania certyfikatów niekwalifikowanych na kartach kryptograficznych zawierających certyfikaty kwalifikowane, ze względu na ryzyko ich przypadkowego usunięcia.

Konfig	juracja usług kr	yptograficznych	×	
\$	KONFI	GURACJA	Q	
U	sługi kryptogra	ificzne:		
	⊖ CSP			
	PKCS #11	C:\Program Files\ENCARD\enigmap11-x64.dll		
			Wybierz	

W trakcie procesu generowania certyfikatu należy wskazać ścieżkę dostępu do posiadanego sterownika PKCS#11. Po wskazaniu pliku sterownika PKCS#11 należy kliknąć *OK* 

🐕 PIN do karty	$\times$
Krajowa Administracja	
Skarbowa Wprowadź PIN do karty kryptograficzne	ej
Parametry karty Token: ENCARD	
SN:         8113550047F9470E           Czytnik:         Athena ASEDrive V3C 0	
PIN: •••••	
OK Anuluj	

Następnie podać kod PIN do karty kryptograficznej i ponownie zatwierdzić OK.

#### PIN jest poufny. Należy zabezpieczyć go w sposób uniemożliwiający dostęp innym osobom.

Certyfikat zostanie wygenerowany i zapisany na karcie. W trakcie operacji zapisu certyfikatu na karcie, konieczne będzie ponowne podanie kodu PIN do karty. Proces ten jest niewizualny i może potrwać kilka minut. W trakcie generowania kluczy zostaje wyświetlony komunikat:

![](_page_16_Picture_10.jpeg)

Po wygenerowaniu certyfikatu jego dane będą prezentowane w oknie "Szczegóły certyfikatu..." aplikacji CertSign.

![](_page_17_Picture_0.jpeg)

🗔 Wybrany certy	fikat do podpisu	
📷 Szczegóły ce	rtyfikatu	Zmień certyfikat
Wystawiony dla:	UID=PL431119218570000, O=PUESC, C=PL, CN= <b>CARA</b> , GIVENNAME= <b>CARA</b> SURNAME= <b>CARA</b> , EMAILADDRESS= <b>CARA</b>	
Wystawione przez:	CN=TEST CCK MF Zewnetrzne, OU=Krajowa Administracja Skarbowa O=Ministerstwo Finansow, C=PL	
Ważny do:	25/08/2023 17:13:26	
Nr seryjny:	270a	

# W kolejnym kroku należy pobrać dokument potwierdzający wydanie certyfikatu. Dokument pobiera się wybierając opcję *Pobierz potwierdzenie*.

CERTYFIKAT NIEKWALIFIKOWANY WYGENEROWANO I ZAINSTALOWA	NO POPRAWNIE	$\times$
Certyfikat celny wydany dia:	o numerze seryjnym 2428 został wygenerowany i zainstalowany poprawnie.	
W celu zakończenia procesu wydania certyfikatu należy pobrać dokument "Po	twierdzenie wydania certyfikatu" używając przycisku "Pobierz potwierdzenie".	
Wygenerowany certyfikat celny można dodatkowo pobrać używając przycisku	"Zapisz certyfikat".	
"Potwierdzenie wydania certyfikatu" można ponownie pobrać w zakładce "Moj	je konto" -> lista certyfikatów celnych -> wybranie właściwego certyfikatu.	
▲ Pobierz potwierdzenie		Zamknij

Dokument potwierdzający wydanie certyfikatu zalecamy wydrukować i przechowywać w bezpiecznym miejscu, ponieważ zawiera on kod pozwalający na zawieszenie lub unieważnienie certyfikatu za pośrednictwem help-desk.

Dokument potwierdzający wydanie certyfikatu oraz część publiczną certyfikatu (bez klucza prywatnego), można pobrać ponownie, zgodnie z opisem w rozdziale 7.

### 4.3. Generowanie certyfikatu przy wykorzystaniu Keystore

Wybranie tej opcji umożliwia przechowywanie kluczy i certyfikatów w zaszyfrowanym pliku na komputerze, oraz proste ich przenoszenie pomiędzy komputerami. Należy jednak mieć na uwadze, że wygenerowane w ten sposób certyfikaty mogą być niewidoczne dla innych aplikacji systemu Windows. Jest to jednocześnie najmniej bezpieczna metoda przechowywania kluczy. Opcję tę można wykorzystywać m.in. w przypadku systemów operacyjnych z rodziny Linux oraz Mac OS X.

Po zaznaczeniu opcji "Keystore" uaktywnią się przyciski: "Utwórz..." oraz "Wybierz...".

ugi kryptograf	czne:			
CSP				
<b>PKCS #11</b>	C:\Program Files\E	EN CARD \enigm	ap11-x64.dll	
				Wybierz
Keystore				
			Utwórz	Wybierz

![](_page_18_Picture_0.jpeg)

Jeśli plik *Keystore* nie został wcześniej utworzony, należy wybrać opcję *"Utwórz…"* (poniżej okna ścieżki do pliku). Jeśli plik *Keystore* był wcześniej utworzony, należy wskazać go przez *"Wybierz…"*. Wybór należy potwierdzić przyciskiem *OK*. Utworzone klucze i certyfikaty zostaną dopisane do tego pliku. Następnie należy wprowadzić hasło chroniące dostęp do kluczy i certyfikatów zapisanych w pliku *Keystore*.

🎋 Nowe	hasło do pliku keystore	$\times$
Krajowa Admin Skarbowa	istracja	
Parame Pike D:\	adź nowe hasło do pliku try _temp_y∖newJKS.jks	
Hasło:	•••••	
Potwierdź ł	nasło: •••••	
	OK Anuluj	

Wprowadzone hasło należy powtórzyć, w celu weryfikacji poprawności, po czym zatwierdzić przyciskiem *OK.* W przypadku gdy wprowadzone hasła będą różne, zwrócony zostanie komunikat błędu. Po poprawnym wpisaniu hasła wyświetli się okno informujące o generowaniu kluczy.

Zalecamy aby hasło było skomplikowane, tzn. składało się z liter małych i wielkich, cyfr oraz znaków specjalnych. Należy zabezpieczyć je w sposób uniemożliwiający dostęp innym osobom.

![](_page_18_Picture_5.jpeg)

Następuje wygenerowanie certyfikatu i przesłanie go na komputer użytkownika. Proces ten jest niewizualny i może potrwać kilka minut. W celu zapisania wygenerowanego certyfikatu należy podać hasło wprowadzone w trakcie generowania klucza prywatnego (1) i zatwierdzić *OK* (2).

Krajowa Administracja Skarbowa	
Wprowadź hasło do pliku Parametry Plik⊂ D:\_temp_y\nevdKS.jks	
Hasło:	

Po wygenerowaniu certyfikatu jego dane zostaną wyświetlone w oknie "*Szczegóły certyfikatu…*" aplikacji CertSign.

![](_page_19_Picture_0.jpeg)

🗟 Wybrany certy	fikat do podpisu	
📷 Szczegóły ce	rtyfikatu	Zmień certyfikat
Wystawiony dla:	UID=PL431119218570000, O=PUESC, C=PL, CN= <b>CARA</b> , GIVENNAME= <b>CARA</b> SURNAME= <b>CARA</b> , EMAILADDRESS= <b>CARA</b>	
Wystawione przez:	CN=TEST CCK MF Zewnetrzne, OU=Krajowa Administracja Skarbowa O=Ministerstwo Finansow, C=PL	
Ważny do:	25/08/2023 17:13:26	
Nr seryjny:	270a	

W kolejnym kroku należy pobrać dokument potwierdzający wydanie certyfikatu. Dokument pobiera się wybierając opcję *Pobierz potwierdzenie*.

![](_page_19_Picture_3.jpeg)

Dokument potwierdzający wydanie certyfikatu zalecamy wydrukować i przechowywać w bezpiecznym miejscu, ponieważ zawiera on kod pozwalający na zawieszenie lub unieważnienie certyfikatu za pośrednictwem help-desk.

Dokument potwierdzający wydanie certyfikatu oraz część publiczną certyfikatu (bez klucza prywatnego), można pobrać ponownie, zgodnie z opisem w rozdziale 7.

![](_page_20_Picture_0.jpeg)

## 5. Wykonanie podpisu elektronicznego

Wykonanie podpisu elektronicznego jest możliwe w trybie online (na stronie PUESC), oraz w trybie offline – lokalnie, poprzez wskazanie plików z dysku komputera. W obu przypadkach aplikacja CertSign musi być uruchomiona, jednak przy podpisywaniu w trybie offline (lokalnym), nie jest konieczne nawiązywanie połączenia ze stroną PUESC.

Przycisk Zmień certyfikat w zakładce Certyfikaty/Log, służy do wybrania certyfikatu podpisującego.

Skarbowa		
Certyfikaty/I	Log 🖉 Podpis	
Nośnik kluc	zy: JKS	
Plik JKS:	C:\Users\digitalized_Desktop\moje_klucze.jks	
🗔 Wybrany ce	rtyfikat do podpisu	
Szczegóły	certyfikatu	Zmień certyfikat
Wystawiony dla:	UID=112233 O=ni OU=ni CN=ni GIVENNAME=ni SURNAME=ni EMATLADDRESS=ni@ni ni	
Wystawione prz	CN=TEST CCK MF Zewnetrzne, OU=Krajowa Administracja Skarbowa O=Ministerstwo Finansow, C=PL	
Ważny do:	08/07/2023 12:41:37	
Nr seryjny:	267a	
oziom logowania 2021-09-07 13:23 2021-09-07 13:23 2021-09-07 13:23 2021-09-07 13:23 2021-09-07 13:23 2021-09-07 13:23 2021-09-07 13:23 2021-09-07 13:24 2021-09-07 13:42	Autodiagnoz     Autodiagnoz     S4.668 INFO Version: 1.3.60     S5.398 INFO EnigmaProvider version: 1.3.60     S5.398 INFO EnigmaProvider version: 1.3.60     S5.405 INFO Default Charset=windows-1250     S6.405 INFO Default Charset=windows-1250     S6.421 INFO Path: pkiApplet     S5.822 INFO HTTPS port: 22413     S5.837 INFO HTTPS port: 22443     S5.837 INFO Running arguments: -n CertSign -t CERTSIGN -I PL -h https://puesc.gov.pl/pki/resource/Instrukcja_Cert     S6.837 INFO WebSocket server started     s3.329 WARN enumCertificatesWithPrivateKeys. alias: MYI/+4LrBb4czbRSeTEF7vPuQizgmU= cert is filtered out!     s3.328 WARN enumCertificatesWithPrivateKeys. alias: MYI/+1544	a Zapisz log Sign.pdf -hv -hed -h

Jeśli w zakładce *Certyfikaty/Log* nie jest wyświetlany żaden certyfikat, należy wybrać *Zmień certyfikat,* zaznaczyć na liście właściwy certyfikat (zostanie on podświetlony), następnie zatwierdzić przyciskiem *OK*.

Wystawiony dla:	Wydany przez:	Termin ważności:	Numer seryjny:	
		20/05/2022 10:25:47	2330	
	CCK MF Zewnetrzne	26/05/2022 08:11:14	1035	
	TEST CCK MF Zewnetrzne	26/05/2022 10:24:15	235b	
, in the second s	TEST CCK MF Zewnetrzne	22/06/2023 09:00:05	2634	
and the second se	TEST CCK MF Zewnetrzne	26/05/2022 10:28:35	235e	
zegóły certyfikatu				
lumer seryjny :				23

![](_page_21_Picture_0.jpeg)

Po wybraniu certyfikatu jego szczegóły zostaną wyświetlone oknie *Szczegóły certyfikatu do podpisów.* **Okno wyboru nie wyświetla certyfikatów, których termin ważności upłynął.** 

W przypadku certyfikatów zapisanych na karcie kryptograficznej i poprawnie zainstalowanych w systemie operacyjnym, wyświetlą się one na liście dopiero **po włożeniu karty do czytnika.** 

Certyfikaty kwalifikowane wykorzystywane w systemie Windows należy uprzednio zarejestrować w systemowym magazynie certyfikatów.

## 5.1 Wykonanie podpisu elektronicznego na PUESC

Wykonanie podpisu elektronicznego możliwe jest po poprawnym wypełnieniu i wygenerowaniu dokumentów na portalu. Podpisanie dokumentów (wniosków, pism) dostępne jest w widoku *Mój Pulpit > Do wysyłki i robocze > Dokumenty do wysyłki*.

Aplikacja CertSign umożliwia złożenie podpisu przy użyciu certyfikatu kwalifikowanego, certyfikatu zawartego w warstwie elektronicznej dowodu osobistego (podpis osobisty) lub certyfikatu celnego (niekwalifikowanego) – w zależności od rodzajów podpisów dopuszczonych dla danego dokumentu. **W przypadku wykorzystywania certyfikatu kwalifikowanego w systemie Windows** - należy zainstalować dostarczone z nim oprogramowanie w komputerze użytkownika, a następnie przeprowadzić proces rejestracji posiadanego certyfikatu kwalifikowanego w systemowym magazynie certyfikatów (zgodnie z dokumentacją certyfikatu kwalifikowanego). Oprogramowanie dostarczane przez polskie centra kwalifikowane z reguły automatycznie instaluje certyfikat kwalifikowany w magazynie certyfikatów systemu Windows.

Analogicznie, **w przypadku wykorzystania podpisu osobistego (danymi w warstwie elektronicznej dowodu osobistego)** należy uprzednio zainstalować i skonfigurować czytnik i oprogramowanie. Opis jest w Dodatku B.

Operacja złożenia podpisu jest możliwa tylko w stosunku do dokumentów, które wcześniej nie zostały podpisane. Dokument niepodpisany oznaczony jest w kolumnie "*Podpisany*" wartością "*Nie*", a dokument podpisany wartością "*Tak*"

W celu złożenia podpisu elektronicznego na dokumencie do wysyłki należy:

a) w zakładce *Do wysyłki i robocze > Do wysyłki,* w pierwszej kolumnie tabeli, za pomocą check-box wskazać dokument do podpisu; następnie wybrać akcję *Podpisz*.

	ETA [	🗊 NAZWA WŁASNA 🛛 💼 USUŃ	🛃 POBIERZ 🧕	WERYF	IKUJ 🅜 PODPISZ	🔺 WYŚLIJ	😋 UDOSTĘPNIJ	0	Nowy dokument
Strona	1							Elementów na	a stronie: 10
		NAZWA DOKUMENTU	:	• N	I AZWA WŁASNA DOK	UMENTU 🏮	PODMIOT TWÓRCA 🏮	DATA UTWORZENIA 韋	PODPISANY 韋
		Elektroniczna forma deklaracji	I INTRASTAT	11 T b x	NTRASTAT_Deklaracji RASTAT_dbdc19e759 319794fe218803aa9 ml	a_AIS_N 9894c99 92bb8df.		2021-08-20 11:36	Tak
		Elektroniczna forma deklaracji	i INTRASTAT	р	lik1.xml			2021-08-20 11:17	Nie

System wyświetli okno z opcją wyboru metody podpisywania dokumentu. Należy zaznaczyć właściwą metodę podpisu i zatwierdzić przyciskiem *Podpisz*.

![](_page_22_Picture_0.jpeg)

PODPIS DOKUMENTU	×
Podpis kwalifikowany     Podpis profilem zaufanym ePUAP     Certyfikat celny	
Podpisz	Anuluj

*Opcje: podpis kwalifikowany, certyfikat celny, podpis osobisty,* spowodują uruchomienie podpisywania w aplikacji CertSign. *Podpis profilem zaufanym ePUAP* przekieruje do serwisu dostawcy podpisu zaufanego.

Wybranie *Podpis kwalifikowany* lub *Certyfikat celny lub Podpis osobisty* uruchomi aplikację CertSign i spowoduje nawiązanie połączenia między stroną PUESC i aplikacją. Ponieważ połączenie nawiązywane jest przez kilka sekund, status połączenia może zmienić się po dłuższej chwili.

![](_page_22_Picture_4.jpeg)

## 5.2 Wykonanie podpisu z certyfikatem w magazynie Windows (CSP)

![](_page_22_Picture_6.jpeg)

Po zatwierdzeniu sposobu dostępu do certyfikatu, aplikacja podpisująca wyświetli dane przeznaczone do podpisu w takiej formie, w jakiej trafiają do SISC.

KAS PO	🎋 Podpisywana treść dokumentu					
	Podpisywana treść dokumentu					
КŗŞ	<pre><?xml version="1.0" encoding="UTF-8"?><ie315 "="" cos="" dataprzybycia="2015-10-26T03:00:00.12" liczbac<="" pre="" xmlns="http://www.mf.gov.pl/xsd/ICS/IE315_v1&lt;br&gt;&lt;DeklaracjaPrzywozowa CRN="></ie315></pre>	L-0.xsd" NrW ^ Dpakowan="44				
	<kontener nr="CBHI"></kontener> <opakowanie liczbaopakowan="22" rodzaj="PK" znaki="No marks"></opakowanie>					
	<pre><miejscedata data="2015-10-26T03:00:00.1Z" miejsce="PL"></miejscedata> </pre>	~				
	<	>				
		dź Anuluj				

Należy potwierdzić prawidłowość wprowadzonych danych przyciskiem *Zatwierdź*. Aplikacja wykona podpis z użyciem wcześniej wskazanego certyfikatu.

Zostanie wyświetlone okno dialogowe, w którym należy podać hasło (PIN), chroniące dostęp do klucza prywatnego. W zależności od sposobu przechowywania certyfikatu i rodzaju samego certyfikatu, możliwe jest pojawienie się następujących okien:

![](_page_23_Picture_0.jpeg)

a) W przypadku certyfikatu celnego zapisanego w systemie Windows i nieznajdującego się na karcie kryptograficznej:

![](_page_23_Picture_2.jpeg)

Należy podać hasło dostępu do certyfikatu (1) i następnie zatwierdzić przyciskiem "OK"(2)".

 b) W przypadku certyfikatu kwalifikowanego, zapisanego na karcie kryptograficznej, zostanie wyświetlone okno dialogowe oprogramowania obsługującego kwalifikowaną kartę kryptograficzną. Okno to może mieć różny wygląd, w zależności od rodzaju posiadanej karty i zainstalowanego oprogramowania do jej obsługi.

Przykładowy widok dla certyfikatu kwalifikowanego wydanego przez polskie centrum certyfikacji

SryptoTech CSP	×		
Сгур	otoCard		
Aktualny proces			
C:\Program Files (x86)\J	ava\jre7\bin\jp2launcher.exe		
Status karty elektroniczn	ei		
Czytnik: OMNIKEY CardMan 3x21 0			
Token:	QESv2 -		
Etykieta klucza:	29ddfd6e73f9a2644fb7c5b343de2b222881		
Numer seryjny:	1012000200125910		
PIN:			
2.			

Należy podać PIN do karty (1) i zatwierdzić przyciskiem "OK" (2). Po przesłaniu podpisanego dokumentu portal PUESC wyświetla komunikat:

INFORMACJA	×
Dokument został poprawnie podpisany.	
	Zamknij

Podpisany dokument prezentowany jest w tabeli dokumentów do wysyłki ze statusem "*Tak*" w kolumnie "*Podpisany*"

![](_page_24_Picture_0.jpeg)

## 5.3 Wykonanie podpisu z karty kryptograficznej zgodnej z PKCS#11

(onfiguracja ເ	usług kr	yptograficznych	×
К	ONFI	GURACJA	$\mathbb{Q}$
Usługi ki	ryptogra	ficzne:	
$\bigcirc$ cs	Р		
🔘 РКС	CS #11	C:\Program Files\ENCARD\enigmap11-x64.dll	
			Wybierz

Aplikacja podpisująca wyświetli dane przeznaczone do podpisu w takiej w formie, w jakiej trafiają do SISC.

K∳ Po	dpisywana treść dokumentu		×
	Podpisyv	vana treść dokumentu	
<b>Қ</b> Ş	xml version="1.0" encoding="UTF-8"? <ie3 <deklaracjaprzywozowa <="" crn="COS " th=""><th>15 xmlns="http://www.mf.gov.pl/xsd/ICS/IE315_v1-0.xsd" NrW DataPrzybycia="2015-10-26T03:00:00.12" LiczbaOpakowan="44</th><th>∦ ^ 4</th></deklaracjaprzywozowa></ie3 	15 xmlns="http://www.mf.gov.pl/xsd/ICS/IE315_v1-0.xsd" NrW DataPrzybycia="2015-10-26T03:00:00.12" LiczbaOpakowan="44	∦ ^ 4
	<kontener nr="CBHL "></kontener> <opakowanie liczbaopakowan="22" rodzaj="PK&lt;/th&gt;&lt;th&gt;" znaki="No marks"></opakowanie>		
	<miejscedata <br="" data="2015-10-26T03:00:00.1Z"></miejscedata>	Miejsce="PLI"/>	~
	<	<u> </u>	
		Zatwierdź Anulu	ıj

Należy potwierdzić prawidłowość wprowadzonych danych przyciskiem Zatwierdź.

Zostanie wyświetlone okno dialogowe, w którym należy podać hasło (PIN), chroniące dostęp do klucza prywatnego. Okno może różnić się wyglądem, w zależności od rodzaju posiadanej karty i zainstalowanego oprogramowania do jej obsługi.

Po poprawnym przesłaniu podpisanego dokumentu portal PUESC wyświetla komunikat:

![](_page_24_Picture_8.jpeg)

Podpisany dokument prezentowany jest w tabeli dokumentów do wysyłki ze statusem "*Tak*" w kolumnie "*Podpisany*"

## 5.4 Wykonanie podpisu z certyfikatem (kluczem) zapisanym w pliku Keystore

Aplikacja korzysta z wybranego pliku *Keystore*, przechowującego klucze i certyfikaty. Podpisywany dokument jest prezentowany w takiej w formie, w jakiej trafia do SISC.

🎋 Po	dpisywana treść dokumentu	>	×
	Podpisyv	vana treść dokumentu	
КŗS	xml version="1.0" encoding="UTF-8"? <ie33 <deklaracjaprzywozowa <="" crn="COS " th=""><th><pre>15 xmlns="http://www.mf.gov.pl/xsd/ICS/IE315_v1-0.xsd" NrW DataPrzybycia="2015-10-26T03:00:00.12" LiczbaOpakowan="44</pre></th><th>^</th></deklaracjaprzywozowa></ie33 	<pre>15 xmlns="http://www.mf.gov.pl/xsd/ICS/IE315_v1-0.xsd" NrW DataPrzybycia="2015-10-26T03:00:00.12" LiczbaOpakowan="44</pre>	^
	<kontener nr="CBHU"></kontener> <opakowanie <="" liczbaopakowan="22" rodzaj="PK" td=""><td>'Znaki="No marks"/&gt;</td><td></td></opakowanie>	'Znaki="No marks"/>	
	<miejscedata <br="" data="2015-10-26T03:00:00.1Z"></miejscedata>	Miejsce="PL"/>	~
	<	>	
		Zatwierdź Anuluj	1

Należy potwierdzić prawidłowość wprowadzonych danych przyciskiem "Zatwierdź".

![](_page_25_Picture_0.jpeg)

Zostanie wyświetlone okno dialogowe, w którym należy podać hasło (PIN), chroniące dostęp do klucza prywatnego.

🐕 Hasło do pliku keystore	$\times$
Krajowa Administracja	
Wprowadź hasło do pliku	
Parametry Plik D:\_temp_y\nevdKS.jks	
Hasło:	
OK Anuluj	

Po poprawnym przesłaniu podpisanego dokumentu portal PUESC wyświetla komunikat:

INFORMACJA	×
Dokument został poprawnie podpisany.	
	Zamknij

Podpisany dokument prezentowany jest w tabeli dokumentów do wysyłki ze statusem "*Tak*" w kolumnie "*Podpisany*"

# 5.5 Wykonanie podpisu elektronicznego lokalnie na komputerze – w trybie offline

Wykonanie podpisu lokalnie polega na wskazaniu, w aplikacji CertSign, położenia pliku do podpisania na dysku komputera. Plik ten może być uprzednio pobrany z PUESC. **W tym przypadku nie jest konieczne połączenie strony PUESC z aplikacją.** 

![](_page_25_Picture_8.jpeg)

By podpisanie pliku było możliwe, w zakładce Certyfikaty/Log powinien być wybrany certyfikat podpisujący.

W zakładce *Podpis* dostępne są funkcje wykonania podpisu elektronicznego. Należy wskazać położenie na dysku komputera pliku, lub plików do podpisania, oraz folderu docelowego; ewentualnie wybrać format i typ podpisu, następnie zatwierdzić operację przyciskiem *Podpisz pliki*.

W menu *Poziom podpisu* ustala się, czy na wskazanym pliku ma być wykonany wyłącznie podpis elektroniczny (poziom "BES") czy też do podpisu ma być dodany elektroniczny znacznik czasu (poziom "T"). W przypadku dodania znacznika czasu konieczne jest wskazanie, w *Ustawieniach,* adresu serwera znacznika czasu (do którego użytkownik ma dostęp).

Dla formularzy przesyłanych na PUESC należy w parametrach podpisu wybrać format podpisu XAdES, typ Otoczony.

Opcja *Sugeruj formaty podpisu* zapewnia automatyczne dostosowanie parametrów, na podstawie typu pliku wybranego do podpisania. Odznaczenie tej opcji odblokowuje możliwość ręcznego ustawiania parametrów.

![](_page_26_Picture_0.jpeg)

## 6. Zgłaszanie problemów, przeglądanie logów

### 6.1 Dane potrzebne do analizy problemów z działaniem aplikacji

- System operacyjny rodzaj i wersja, wersja językowa systemu (np.: Windows 10 wersja Polska)
- Rodzaj i wersja przeglądarki internetowej
- Log z konsoli aplikacji CertSign
- Widok ekranu z błędem cały ekran (przycisk klawiaturowy PrtScr)
- Dokładny opis problemu, okoliczności wystąpienia.
- Wynik autodiagnozy aplikacji.

## 6.2 Włączanie logowania w aplikacji CertSign

Aplikacja CertSign umożliwia włączenie "pełnego" logowania zdarzeń z działania aplikacji. W celu uruchomienia pełnego logowania należy w oknie aplikacji przestawić Poziom logowania na "Pełny".

Poziom logowania: O Prosty O Pełny

Autodiagnoza Zapisz log

W oknie poniżej zaczną wyświetlać się logi z działania aplikacji, które można zapisać klikając przycisk "Zapisz log"

Zapisane logi w przypadku błędów należy załączyć do zgłoszenia w HELPDESK.

![](_page_27_Picture_0.jpeg)

## 7. Pobranie certyfikatu lub dokumentu potwierdzenia z konta na PUESC

Dedykowany widok certyfikatów celnych na PUESC jest dostępny z bocznego menu w widoku Mój pulpit > Moje dane > Certyfikaty celne. Składa się on z dwóch głównych obszarów:

- Lista certyfikatów celnych użytkownika w tej części widoku użytkownik ma możliwość przeglądania listy swoich certyfikatów celnych. Klikając w wyróżniony na czerwono numer seryjny, użytkownik ma możliwość podglądu certyfikatu oraz jego pobrania.
- Dodatkowe pliki sekcja ta zawiera certyfikaty do pobrania oraz dokumentację związaną z certyfikatami.

tyfikaty Co TA CERTYFIK	elne ATÓW CELNY	сн		Pokaż dane w SISC  MOJE DANE MOJE SZCZEGÓŁOWE DANE
nie zawiera certyfikato	ów kwalifikowanych ora WAŻNY OD:	z kluczy do bezpiecznej trar WAŻNY DO:	nsmisji danych wydanych przez IC Kraków AKCJE:	WYSZUKAJ PODMIOT     AKTUALIZUJ DANE UŻYTKOWNIKA
1e199	2020-10-19	2022-10-19	Zawieś Odwieś Unieważnij	> LISIA REPREZENTOWANYCH PODMIOTOW
1e31d	2020-10-28	2022-10-28	Zawieś Odwieś Unieważnij	
1f78f	2021-03-22	2023-03-22	Zawieś Odwieś Unieważnij	
tyfikaty:	Gé	neruj certyfikat celny		
K_MF_Infrastruktura_i_	Aplikacje.crt			
K_MF_Root.crt				
K_MF_Wewnetrzne.crt				

W celu pobrania certyfikatu, lub dokumentu potwierdzenia wydania certyfikatu, należy kliknąć na nr seryjny certyfikatu. Zostanie wyświetlone okno:

	CERTYFIKAT 2219	<
	BEGIN CERTIFICATEMIIEbDCCA15gAwlBAgICIhkwDQYJKoZIhvcNAQELBQAwdzELMAkGA1UEBhMCUEwxHjAcBgNVBAoMFU1pbmIzdGVyc3R3byBGaWShbnNvdzEnMCU GA1UECwwe53Jham93YSBBZG1pbmIzdHjhY2phIFNrYXJjb3dhMR8wHQYDVQQDDBZURVNUIENDSyBNRiBaZXduZXRyemSIMB4XDTE5MTAyNzA4NDUzNicXDTixMTAyNjA4NDU zNiowgaExizAhBgkqhkiG9w0BCQEWFGphbi50aGVvcGhpbHVzQHdwLhBsMRMwEQYDVQQEDAp0aGVvcGhpbHVzMQwwCgYDVQQqDANqYW4xFz4VBgNVBAMMDmphbiB0aG VvcGhpbHVzMQswCQYDVQQEwjQTDE0MAwGA1UECgwFUFVFU0Mx1TAf8gojkiajk/JsZAEBDBFQTDM0MDIxMjk3NjMSMDAwMDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC AQoCggEBAMKtLej6UA-EfinHuPMJ99XUokDerM4XrMQxRm15Y48hnF5A6gy204Bf2E902Cz82G1+SER5gmjjTVR9ueuC99tuMUrjgo/zr5bHCfa5XLv2Z5h9CBb50pU2VFFAVK2JSU6 ghxITVS-ORKZa+BXjDmVdIMVWtGvJ9cwBrfEgJAoK4pNd1MVmKVPH626M78XYcLdcalhDk0T5PreoNE2Y2pE7LqbKRW9XrJGOnQ9V8NXIEb7we7Vij05XMkPQ99QiKARZ5LV38 mEpNT5s9W9IiwLn/a~w6d3IIQu1QM/CubIqFN6xp2/vn1T8xZJF0+tdw2PduRrMfXXId2sRXg0CAwEAAa081jCB0z4MBgNVHRMBAREAjAAMB0GA1UdDgQWBBSy9ATmUVm+0C Oq6h22D5oTC4CaFTAOBgNVHQ8Baf8EBAMCB4AwFgYDVR0IAQH/BAwwCgYIKwYBBQUHAwQwPwYIKwYBBQUHAQEEMzAxMC8GCCsGAQUFBzABhiNodHRwOi8vdGVzdG9ic3 Bwa2lzYy5tZi5nb3YucGwr0NTUDDA7BgNVHR8EDAM/CQLqAshipodHRwczovL3812XNJLmdvdi5wbC9wa2kvY3JsL3Ric3RtZnpIdy5jcmwDQVJKoZIhvcNAQELBQADggEBALY Shp~MbYAdd0JSiCFgurinaW7T+Bq8c9Q7bBM/rRL5csHHpSwnRZn2h0T20V5UNgg6biKP1wHT1wHETr9dwrZRWXjSWv7UJLs8+aExsh3LXVDZsGa+OUCQRniqzQE/6IpoqVuxgHp5g01pB FV+VAU6GPXdkj56jAkrt/0FVhSHFKiKXF+koi3w0ioyQF8WUwScSkDqb0yD0ASUU=END CERTIFICATE	JUGCJ6RC3Y8B
3	1     2       Poblerz potwierdzenie     Zapisz certyfikat	

W celu pobrania dokumentu potwierdzającego należy kliknąć przycisk *Pobierz potwierdzenie* (1). W celu pobrania certyfikatu (części publicznej) należy kliknąć przycisk *Zapisz certyfikat* (2).

UWAGA! Pobrana zostanie tylko część publiczna certyfikatu. Część prywatna nie jest przechowywana w SISC i nie jest możliwe jej odzyskanie.

![](_page_28_Picture_0.jpeg)

## 8. Aktualizacja aplikacji CertSign

Aplikacja CertSign posiada wbudowany mechanizm sprawdzania aktualizacji. Po stwierdzeniu dostępności aktualizacji zostanie wyświetlony komunikat z propozycją jej pobrania. Możliwe jest pobranie aktualizacji lub rezygnacja (anulowanie). W przypadku pobrania aktualizacji instalator zaproponuje jej zainstalowanie. Instalację można wykonać od razu lub odłożyć na później. Instalacja nowej wersji nie kasuje ustawień dotyczących certyfikatu użytkownika.

![](_page_29_Picture_0.jpeg)

## 9. Dodatek A

## A.1 Manualna instalacja certyfikatów w systemie Windows

W celu poprawnej weryfikacji certyfikatów celnych konieczne jest zainstalowanie w systemie certyfikatów centrów certyfikacji, do których odnośniki znajdują się na https://puesc.gov.pl/uslugi/uzyskaj-lub-uniewaznij-certyfikat-celny

Aby zainstalować certyfikaty Centrum Certyfikacji MF należy w wyświetlonym widoku odszukać i pobrać na komputer certyfikaty:

- CCK MF Root,
- CCK MF Zewnetrzne,
- CCK MF Wewnetrzne,
- CCK MF Infrastruktura i Aplikacje

Po pobraniu pliku certyfikatu należy na nim dwukrotnie kliknąć – spowoduje to wyświetlenie okna prezentującego certyfikat. Następnie kliknąć przycisk "Zainstaluj certyfikat"

goine	Szczegóły	Ścieżka certyfikacji	
1	Inform:	acje o certyfikacie	
Ten	certyfikat	jest przeznaczony do:	
	<ul><li>Wszystki</li><li>Wszystki</li></ul>	e zasady wydawania e zasady aplikacji	
Wy	stawiony d	lla: Centrum Certyfikad	iji Ministerstwa Finansow
Wy	stawiony p	rzez: Centrum Certyfikad	cji Ministerstwa Finansow
Wa	żny od 20:	17-05-10 <b>do</b> 2040-05-04	4
		Zainstalui certyfikat	Oświadczenie wystawcy
		Zainstaluj certyfikat	Oświadczenie wystawcy

Zostanie uruchomiony "Kreator importu certyfikatów".

![](_page_29_Picture_12.jpeg)

W oknie należy wybrać przycisk "Dalej".

W kolejnym oknie należy zaznaczyć opcję "Umieść wszystkie certyfikaty w następującym magazynie"(1), następnie wybrać "Przeglądaj" (2).

![](_page_30_Picture_0.jpeg)

Magazyn certyfikatów	
Magazyny certyfikatów to obszary system certyfikaty.	nowe, w których przechowywane są
System Windows może automatycznie wyl określić inną lokalizację dla certyfikatu.	brać magazyn certyfikatów; możesz jednak
🔘 Automatycznie wybierz magazyn ce	ertyfikatów na podstawie typu certyfikatu
(a) Umioóć wazyatkie contyfikaty w paci	
Magazyn certyfikatów:	tępującym magazynie
Umieść wszystkie certyfikaty w nasi Magazyn certyfikatów:     Dowiedz się więcej o <u>magazynach certyfikatów</u>	Przeglądaj

Certyfikat CCK MF Root należy umieszczać w magazynie "Zaufane główne urzędy certyfikacji". Certyfikaty CCK MF Zewnetrzne, CCK MF Wewnetrzne, CCK MF Infrastruktura i Aplikacje należy umieszczać w magazynie "Pośrednie urzędy certyfikacji"

W dalszej części pokazane zostały widoki ekranów dla procesu instalacji certyfikatu CCK MF Root.

1. Otworzy się okno wyboru magazynu certyfikatów.

Mag	<b>azyn certyfikatów</b> Magazyny certyfikatów to obszary systemowe, w których przechowywane są
	ertyfikaty. Wybieranie magazynu certyfikatów katów; możesz jednak
Dowi	Wybierz magazyn certyfikatów, którego chcesz użyć. Osobisty Zaufanie główne urzędy certyfikacji Zaufanie przedsiębiorstwa Pośrednie urzędy certyfikacji Szufani wydawcy Certyfikaty niezaufane Główne urzędy certyfikacji Pokaż magazyny fizyczne 2. OK Anuluj
	< Wstecz Dalej > Anuluj

Należy wybrać *Zaufane główne urzędy certyfikacji* (1) i zatwierdzić wybór przyciskiem *OK* (2). Kontynuować zatwierdzając przyciskiem *Dalej.* 

	м	lagazyn cert	yfikatów:			
		Zaufane głó	wne urzędy certy	yfikacji		Przeglądaj
			1	11		
owied:	lz się v	więcej o <u>mag</u>	azynach certyfik	atów	_	_
owied	lz się v	więcej o <u>mag</u>	azynach certyfik	<u>atów</u>		1
owied:	lz się v	więcej o <u>mag</u>	azynach certyfik	<u>atów</u>	Ļ	Ļ
owied:	lz się v	więcej o <u>mag</u>	azynach certyfik	<u>atów</u>	 ſ	ֈ

![](_page_31_Picture_0.jpeg)

W oknie Kończenie pracy kreatora importu certyfikatów wybrać Zakończ.

Kreator importu certyfikatów	×
	Kończenie pracy Kreatora importu certyfikatów
	Certyfikat zostanie zaimportowany po kliknięciu przycisku Zakończ.
	Wybrane zostały następujące ustawienia:
	Magazyn certyfikatów wybrany przez użytkownika Zaufa
	Zawartosc Certy
	< Wstecz Zakończ Anuluj

Po poprawnym zakończeniu importu certyfikatu pojawia się komunikat:

Kreator importu certyfikatów	K J
import został pomyślnie ukończony.	
ОК	

Procedurę należy powtórzyć dla pozostałych certyfikatów CCK MF.

## A.2 Weryfikacja poprawności certyfikatu osobistego w systemie Windows

W celu sprawdzenia poprawności zainstalowanego w systemie Windows certyfikatu osobistego można uruchomić przeglądarkę Internet Explorer, następnie wybrać *Narzędzia > Opcje internetowe > Zawartość > Certyfikaty* 

Podgląd magazynu certyfikatów można wywołać również z przeglądarki Edge, wybierając Ustawienia > Prywatność, wyszukiwanie i usługi > Zabezpieczenia > Zarządzaj certyfikatami

![](_page_31_Picture_9.jpeg)

Trzecią możliwością (dla zaawansowanych użytkowników) jest uruchomienie systemowej konsoli *mmc*, dodanie przystawki *Certyfikaty – bieżący użytkownik* i wyświetlenie certyfikatów w gałęzi *Osobisty*.

![](_page_31_Picture_11.jpeg)

![](_page_32_Picture_0.jpeg)

W celu przeglądania wybranego certyfikatu należy kliknąć go dwukrotnie. Otwarty zostanie widok zawartości. W przypadku <u>certyfikatu osobistego</u> na pierwszej zakładce powinien znajdować się napis "**Masz klucz prywatny, który odpowiada temu certyfikatowi**". Brak klucza prywatnego uniemożliwia złożenie podpisu elektronicznego.

🔲 Cer	tyfikat	2
Ogólne	Szczegóły Ścieżka certyfikacji	
1,10	Informacje o certyfikacie	
Ter	n certyfikat jest przeznaczony do:	
	• Zabezpiecza wiadomości e-mail	
wy	stawiony dla:	
wy	stawiony przez: CCK MF Zewnetrzne	
Wa	żny od 2017-05-12 do 2019-05-12	
1	Masz klucz prywatny, który odpowiada temu certyfikatowi.	
	Oświadczenie wystawo	/
	ок	

Następnie należy przejść na zakładkę Ścieżka certyfikacji. W przypadku poprawnej instalacji certyfikatów, w wyświetlonym oknie będą znajdowały się certyfikaty centrum certyfikacji oraz certyfikat osobisty.

🤁 Certyfikat	×
Ogólne Szczegóły Ścieżka certyfikacji	
Ścieżka certyfikacji	
Centrum Certyfikacji Ministerstwa Finansow	
Wyświetl certyfika	it
Stan certyfikatu:	
Ten certyfikat jest prawidłowy.	
C	)K

Jeśli na ikonie certyfikatów powyżej certyfikatu osobistego znajduje się dodatkowy znak ("x" w czerwonym kole), oznacza to, że ten certyfikat nie został zainstalowany lub jest nieprawidłowy i ścieżka certyfikacji nie może zostać poprawnie zbudowana. Należy w takiej sytuacji pobrać i zainstalować brakujący certyfikat.

## A.3 Eksport certyfikatu z magazynu certyfikatów systemu Windows

W celu wyeksportowania certyfikatu zainstalowanego w magazynie systemu Windows (CSP) należy wyświetlić magazyn certyfikatów poprzez przeglądarkę Internet Explorer (*Narzędzia > Opcje internetowe > Zawartość > Certyfikaty*) lub przeglądarkę Edge (*Ustawienia > Prywatność, wyszukiwanie i usługi > Zabezpieczenia > Zarządzaj certyfikatami*) – analogicznie jak opisano we wstępie do A.2.

![](_page_33_Picture_0.jpeg)

W oknie *Certyfikaty* na zakładce *Osobisty* należy zaznaczyć certyfikat do eksportu (1), a następnie kliknąć przycisk *Eksportuj* (2)

ertyfikaty	i have			X
Zamierzony cel:	<wszyscy></wszyscy>			-
Osobisty Inne oso	by Pośrednie urzędy certy	yfikacji Zaufa	ne główne urzędy o	ertyfikacji 🚺 🕨
Wystawiony dla	Wystawiony przez	Data wyg	Przyjazna nazwa	1
🛱 Paweł	Testowe Centrum Cer	2017-04-16	Pawel	
			-	·
Importuj Eks	sportuj Usuń		Za	awansowane
Zamierzone cele cer	tyfikatu			
Bezpieczna poczta e	-mail <b>2.</b>			
				wyswieti
			_	

Zostanie wyświetlone okno Kreatora eksportu certyfikatów

![](_page_33_Picture_4.jpeg)

#### Następnie należy kliknąć przycisk Dalej

W oknie Eksportu klucza prywatnego należy zaznaczyć opcję Tak, eksportuj klucz prywatny (1)

Następnie należy kliknąć przycisk Dalej (2)

![](_page_34_Picture_0.jpeg)

Jeśli certyfikat ma być nadal użytkowany na komputerze, z którego jest eksportowany, należy zaznaczyć opcje jak na widoku poniżej. W przeciwnym wypadku należy także zaznaczyć opcję *Usuń klucz prywatny* ...

Format pliku eksportu Certyfikaty mogą być eksportowane w wielu różnych formatach plików.		
v	/ybierz format, którego chcesz użyć:	
	Certyfikat X.509 szyfrowany binarnie algorytmem DER (.CER)	
	Certyfikat X.509 szyfrowany algorytmem Base-64 (.CER)	
	💿 Standard składni wiadomości kryptograficznych - certyfikaty PKCS #7 (.P7B)	
	🗌 Jeżeli jest to możliwe, dołącz wszystkie certyfikaty do ścieżki certyfikacji	
	Wymiana informacji osobistych - PKCS #12 (.PFX)	
	📝 Jeżeli jest to możliwe, dołącz wszystkie certyfikaty do ścieżki certyfikacji	
	🔲 Usuń klucz prywatny, jeżeli eksport został zakończony pomyślnie	
	Eksportuj wszystkie właściwości rozszerzone	
	🔘 Magazyn certyfikatów seryjnych firmy Microsoft (.SST)	
Dowie	dz się więcej o <u>formatach plików certyfikatów</u>	
	< Wstecz Dalej > Anuluj	

Następnie należy kliknąć przycisk *Dalej.* W kolejnym kroku należy ustawić hasło zabezpieczające eksportowany certyfikat (1) oraz kliknąć przycisk *Dalej.* 

	0
	Aby zapewnić bezpieczeństwo, musisz zabezpieczyć klucz prywatny za pomocą hasła.
	Wpisz i potwierdź hasło.
	Hasło:
-	••••••
~	Wpisz i potwierdź hasło (obowiązkowe):
	······

W kolejnym kroku podać nazwę pliku, do którego zostanie wyeksportowany certyfikat i wybrać Dalej.

Eksport pliku	
Określ nazwę pliku, który chcesz	z wyeksportować
Nazwa pliku:	
Nazwa pliku: C:\certyfikat.pfx	Przeglądaj

![](_page_35_Picture_0.jpeg)

W celu zakończenia procesy należy kliknąć przycisk Zakończ.

Kreator eksportu certyfikatów		x
	Kończenie pracy Kreatora eksportu certyfikatów	
<u>_</u>	Praca Kreatora eksportu certyfikatów została pomyślnie ukończona. Wybrane zostały następujące ustawienia:	
	Nazwa pliku C: Klucze eksportu Tał Dołącz wszystkie certyfikaty ze ścieżki certyfikacji Tał Format pliku Wy	
	4	
	< Wstecz Zakończ Anuluj	

System rozpocznie eksportowanie certyfikatu i wyświetli okno z pytaniem o hasło, którym jest zabezpieczony klucz prywatny. Jest to hasło, które zostało podane w momencie generowania certyfikatu - **nie jest to hasło podawane w kroku** *"hasło zabezpieczające eksportowany certyfikat"*.

Eksportowanie	: prywatnego klucza wymiany
	Aplikacja żąda dostępu do elementu chronionego.
	Hasło dla: Klucz prywatny CryptoAPI
	OK Anuluj Szczegóły

Należy podać poprawne hasło (1) i kliknąć przycisk OK. (2)

Jeśli zostało podane poprawne hasło, certyfikat zostanie wyeksportowany i zapisany we wskazanym pliku, a system wyświetli komunikat potwierdzający:

ſ	Kreator eksportu certyfikatów
	Eksport zakończył się pomyślnie.
	ОК

![](_page_36_Picture_0.jpeg)

## A.4 Import certyfikatu do magazynu certyfikatów systemu Windows (CSP)

W celu zaimportowania uprzednio wyeksportowanego certyfikatu, należy zaznaczyć plik \*.pfx (lub \*.p12) z wyeksportowanym certyfikatem i kliknąć prawy przycisk myszy

![](_page_36_Picture_3.jpeg)

Zostanie wyświetlone menu, z którego należy wybrać: "Zainstaluj PFX"

![](_page_36_Picture_5.jpeg)

Następnie należy kliknąć przycisk Dalej. Zostanie wyświetlone okno Kreatora importu certyfikatów

Kreator importu cer	tyfikatów
Import pliku	
Wybierz plik,	który chcesz zaimportować.
Nazwa pliku:	1.
C:\certyfika	t.pfx Przeglądaj
Uwaga: użyv w pojedyncz	ając następujących formatów, można przechować więcej niż jeden certyfikat /m pliku:
Wymiana	nformacji osobistych- PKCS #12 (.PFX,.P12)
Standard	składni wiadomości kryptograficznych - certyfikaty PKCS #7 (.P7B)
Magazyn	zertyfikatów seryjnych firmy Microsoft (.SST) 2.
Dowiedz się więce	j o <u>formatach plików certyfikatów</u>
	< Wstecz Dalej > Anuluj

W polu *nazwa pliku* zostanie automatycznie wpisana ścieżka do pliku z wyeksportowanym certyfikatem. Jeśli pole jest puste, należy wskazać w nim plik z wyeksportowanym certyfikatem (1) i następnie kliknąć przycisk *Dalej* (2)

Zostanie wyświetlone okno z pytaniem o hasło zabezpieczające eksportowany certyfikat (1) – hasło zostało podawane w trakcie eksportu certyfikatu w oknie *Hasło* – kreatora eksportu certyfikatów.

![](_page_37_Picture_0.jpeg)

Jeżeli chcemy umożliwić dalszy eksport certyfikatu w przyszłości należy zaznaczyć opcję Oznacz ten klucz jako eksportowany ... (aczkolwiek kolejne eksporty stanowią dodatkowe ryzyko utraty kontroli nad kluczem prywatnym, więc nie należy nadużywać tej opcji).)

Hasło W celu zapewnienia bezpieczeństwa klucz prywatny jest chroniony hasłem. Wpisz hasło dla klucza prywatnego. Hasło:
W celu zapewnienia bezpieczeństwa klucz prywatny jest chroniony hasłem. Wpisz hasło dla klucza prywatnego. Hasło:
Wpisz hasło dla klucza prywatnego. Hasło:
Włącz silną ochronę klucza prywatnego. W przypadku wybrania tej opcji użytkownik będzie informowany o każdym użyciu klucza prywatnego przez aplikacie.
Oznacz ten klucz jako eksportowalny. Pozwoli to na późniejsze wykonanie kopii zapasowej lub transport kluczy.
Dołącz wszystkie właściwości rozszerzone
Dowiedz się więcej o <u>ochronie kluczy prywatnych</u>
< Wstecz Dalej > Anuluj

Następnie należy kliknąć przycisk *Dalej*. Zostanie wyświetlone okno wyboru magazynu certyfikatów w systemie Windows.

![](_page_37_Figure_4.jpeg)

Należy zaznaczyć opcję *Umieść wszystkie certyfikaty w następującym magazynie* (1), następnie wybrać *Przeglądaj* (2). Otworzy się okno wyboru magazynu certyfikatów, gdzie należy wybrać <u>Osobisty</u> (3). Następnie kliknąć przycisk *OK* (4) i przycisk *Dalej* (5)

![](_page_38_Picture_0.jpeg)

certyfikatów	porta
Certyfikat zostanie zaimportowany po kliknie Zakończ.	ciu przycisku
Wybrane zostały następujące ustawienia:	
Magazyn certyfikatów wybrany przez użyt	kownika Osob
Zawartość	PFX
Nazwa pliku	C: \Us
•	÷.

W celu zakończenia procesu należy kliknąć przycisk Zakończ.

Po poprawnym zakończeniu procesu importu certyfikatu zostanie wyświetlone okno z potwierdzeniem zakończenia procesu.

Kreator importu certyfikatów	X
import został pom	yślnie ukończony.
	ОК

Należy kliknąć przycisk *OK*. Po zakończeniu procesu importu certyfikatu należy zweryfikować jego poprawność zgodnie z procedurą opisaną w Dodatku A.2. Jeśli konieczne jest doinstalowanie certyfikatów centrum certyfikacji, należy postępować zgodnie z instrukcjami z Dodatku A.1.

## A.5 Opis opcji Konfiguracja usług kryptograficznych

- CSP domyślny sposób przechowywania certyfikatów w systemie Windows. Certyfikaty zapisane w systemie Windows umożliwiają wyeksportowanie ich i zainstalowanie na innym komputerze. Jeżeli w systemie Windows zainstalowano uprzednio sterowniki karty kryptograficznej, zgodne ze standardem CSP, możliwe będzie generowanie kluczy i zapisanie certyfikatu bezpośrednio na karcie kryptograficznej użytkownika. Jeśli aplikacja do generowania certyfikatów nigdy nie była uruchamiana, opcja CSP jest domyślnie wybrana.
- 2. PKCS#11 standard dla kart kryptograficznych, alternatywny sposób przechowywania certyfikatów, niezależny od posiadanego systemu operacyjnego. Może mieć zastosowanie między innymi w systemie Linux. Wygenerowany certyfikat zostanie zapisany na karcie kryptograficznej zgodnej z PKCS#11. Jest to najbezpieczniejsza metoda przechowywania kluczy kryptograficznych i certyfikatu, umożliwiająca wykorzystanie certyfikatu na wielu komputerach. W procesie konfiguracji konieczne będzie wskazanie lokalizacji sterownika PKCS#11 (informacje o tym powinny być uprzednio dostarczone przez producenta lub dystrybutora posiadanej karty kryptograficznej).
- 3. Keystore alternatywny sposób przechowywania certyfikatów, obsługiwany przez mechanizmy Java™ (JKS Java KeyStore). Metoda ta jest niezależna od posiadanego systemu operacyjnego. Należy mieć na uwadze, że wygenerowane w ten sposób certyfikaty mogą być niewidoczne dla aplikacji systemu Windows.

![](_page_39_Picture_0.jpeg)

## A.6 Rozwiązanie problemów z połączeniem strony PUESC z aplikacją CertSign

Strona PUESC nawiązuje połączenie z CertSign **w czasie generowania certyfikatu lub podpisywania dokumentu**. W pozostałym czasie CertSign wskazuje status brak połączenia, co jest sytuacją normalną. Główne przyczyny braku połączenia podczas generowania certyfikatu lub podpisywania dokumentu na PUESC (w trybie online) to brak certyfikatów CCK MF lub blokowanie połączeń localhost przez zaporę Windows, oprogramowanie antywirusowe lub inne mechanizmy zabezpieczeń. Mogą zdarzyć się specyficzne sytuacje, związane z indywidualną konfiguracją komputera czy oprogramowania.

W przeglądarce Chrome może wystąpić problem z połączeniem przeglądarki z aplikacją CertSign Rozwiązaniem jest zmiana w konfiguracji przeglądarki. Należy wejść w zaawansowane opcje Chrome, wpisując w pasku adresu: *chrome://flags/#allow-insecure-localhost* i ustawić wartość na *Enabled*.

1	agy allow insectie locarlost		
	Q Search flags		Rese
•	Allow invalid certificates for resources loaded from localhost.		
	Allow invalid certificates for resources loaded from localhost. Allows requests to localhost over HTTPS even when an invalid certificate is presented. – Mac, Windows, Linux, Chrome OS, Android, Fuchsia	Enabl	ed

Następnie należy ponownie uruchomić przeglądarkę.

## A.7 Weryfikacja poprawności podpisu na portalu PUESC

W celu zweryfikowania poprawności podpisu na PUESC należy:

- 1. Wybrać dokument z *Mój pulpit > Do wysyłki i robocze*, klikając jego nazwę.
- 2. Wybrać akcję Weryfikuj podpis.

PUESC > Mój pulpit > Do wysyłki i robocze >

![](_page_39_Picture_11.jpeg)

Po wybraniu akcji system zweryfikuje poprawność podpisu i wyświetli komunikat z wynikiem weryfikacji.

PUESC udostępnia również dedykowaną usługę **Zweryfikuj podpis elektroniczny** w sekcji **Elektroniczne podpisywanie dokumentów**, dostępną też poprzez kafelek na stronie głównej.

![](_page_39_Picture_14.jpeg)

![](_page_40_Picture_0.jpeg)

## **Dodatek B**

## B.1 Podpisanie danymi z warstwy elektronicznej dowodu osobistego

Aplikacja od wersji 1.3.60 obsługuje wykonywanie podpisów z wykorzystaniem danych warstwy elektronicznej dowodu osobistego. Aby wykonać podpis osobisty należy uprzednio zainstalować oprogramowanie *E-dowód menedżer* oraz *E-dowód podpis elektroniczny*. Więcej informacji o e-dowodzie na stronie <u>https://www.gov.pl/web/e-dowod</u>

Przed wykonaniem podpisu, w aplikacji *E-dowód Menedżer* powinien być odblokowany PIN certyfikatu do podpisu osobistego:

	Seria i num Data ważn	ner dowodu: ości:		
15	lmiona: Nazwisko:	``````````````````````````````````````		j.
Certyfikat identyfika uwierzytel	do cji i niania	Certyfikat do podpisu osobistego	Certyfikat do potwierdzania obecności	Certyfikat kwalifikowany
Możesz poti swoją tożsc internecie (i korzystać z	wierdzać Imość w na przykład e-usług)	Možesz podpisywać dokumenty (służy jako elektroniczny podpis)	Możesz potwierdzać swoją obecność (na przykład w placówce medycznej)	Możesz dodawać certyfikaty kwalifikowane
$( \rightarrow )$		$( \rightarrow )$	$(\rightarrow)$	

Jeśli PIN tego certyfikatu jest odblokowany, można dokonywać podpisów cyfrowych.

Sposób wykonania podpisu z użyciem CertSign jest taki jak dla innych nośników PKCS#11. Należy w konfiguracji usług kryptograficznych wskazać odpowiednią bibliotekę i token do podpisu, analogicznie jak opisano w rozdziale 5.3. Biblioteki PKCS#11 znajdują się w folderze instalacyjnym aplikacji *E-dowód Menedżer*. Należy wybrać wersję dostosowaną do posiadanej platformy, tzn. w przypadku architektury 32bitowej oraz 32-bitowej dystrybucji CertSign, należy wskazać 32-bitową bibliotekę *e-dowod-pkcs11-32.dll,* jak na poniższym widoku:

![](_page_41_Picture_0.jpeg)

<b>C</b>	JURACJA		
ługi kryptogr	aficzne:		
⊖ CSP			
<b>● PKCS #11</b>	C:\Program Files\PWPW\e-dov	wod\32\e-dowod-pkcs11-32.dll	
			Wybierz
◯ Keystore			

W kolejnym kroku należy wybrać token do podpisu. Domyślnie do podpisów stosuje się token **Authorization**, zawierający certyfikat do podpisu osobistego.

👫 Wybór	urządzenia		×	
Dostępne	urządzenia			
Czytnik	Identive CLOUD 4700 F Contact	ess Reader 0 #4	2] ~	
Param Nume	etry karty Token: E-Dowód (Authorization er seryjny: <brak></brak>	ı) #42		
Krajowa Skarbowa	Administracja	ОК	Anuluj	

Kolejne operacje wykonuje się zgodnie z opisem w rozdziale 5.3.

## B.2 Funkcje skalowania elementów interfejsu graficznego

Aplikacja od wersji 1.3.60 umożliwia skalowanie czcionek ekranowych do trzech rozmiarów:

- standardowy
- większy
- największy

Aby zmienić rozmiar czcionek należy wybrać jeden z przycisków skalowania, który nie jest aktualnie wybrany. Każdy kolejny rozmiar jest większy od poprzedniego półtorakrotnie. Oznacza to, że powiększenie rozmiaru *standardowego* do *większego* skutkuje wzrostem aktualnego rozmiaru czcionek o 150%, zaś do największego – o 225%. Tak samo, zmniejszenie z *największego* do *większego* zmniejszy poziom z 225% rozmiaru *standardowego* do 150%, a ponowny powrót do *standardowego* pomniejszy aktualny poziom półtorakrotnie, czyli powrót do 100%.

Kolejność skalowania nie ma znaczenia - można jej dokonywać w dowolnej kolejności.

![](_page_42_Picture_0.jpeg)

![](_page_42_Picture_1.jpeg)

Przyciski powiększania czcionek są zaznaczone czerwoną ramką na powyższym widoku ekranu.

W przypadku wyświetlaczy o niższych rozdzielczościach aplikacja może blokować częściowo lub całkowicie możliwość skalowania, w celu uniknięcia błędów przeskalowania elementów interfejsu aplikacji.

## B.3 Obsługa aplikacji przez czytnik ekranu

Aplikacja od wersji 1.3.60 jest przystosowana do obsługi przez czytnik NVDA dla Windows oraz VoiceOver dla macOS.

Domyślna konfiguracja aplikacji VoiceOver jest dostosowana do operowania klawiaturą. Wówczas, istnieje możliwość przechodzenia klawiszem *Tab* po kolejnych komponentach i ich odczytywanie bądź wybieranie. Jeśli jakiś komponent nie jest osiągalny klawiszem *Tab*, można wciąż przesuwać kursor programu VoiceOver za pomocą przycisków lewej oraz prawej strzałki na klawiaturze.

Jeśli jednak istnieje potrzeba, by każdy tekst był odczytywany przy najeżdżaniu na niego myszką, należy w ustawieniach programu VoiceOver wybrać opcję Synchronizuj fokus klawiatury i kursor VoiceOver.

![](_page_42_Picture_8.jpeg)

Wówczas, kursor VoiceOver będzie ustawiany za pomocą najechania kursorem myszki na obiekt.

## B.4 Nawigowanie i sterowanie klawiaturą

Aplikacja CertSign może być obsługiwana przy użyciu klawiatury. Przemieszczanie po kolejnych elementach realizowane jest klawiszem Tab. Cofanie można wykonać kombinacją Shift + Tab

W celu wybrania innej zakładki za pomocą klawiatury, mając wybrany pierwszy element można przechodzić w przód i w tył kombinacjami odpowiednio Ctrl + Tab oraz Shift + Ctrl + Tab.

Więcej wskazówek oraz domyślnych skrótów klawiszowych można znaleźć pod tym adresem https://www.ibm.com/docs/en/sdk-java-technology/8?topic=applications-default-swing-key-bindings

![](_page_43_Picture_0.jpeg)

#### Obsługa obiektu typu ComboBox (lista rozwijana)

Aby wyświetlić listę elementów do wybrania, po najechaniu na obiekt typu ComboBox wcisnąć:

- Na Windows: Alt + strzałka w dół
- Na Linux oraz MacOS: Spację

Aby wybrać inny element, należy zjechać w odpowiednią stronę strzałką w górę lub w dół. Aby natychmiastowo wybrać dany element, należy przy rozwiniętej liście wybrać klawisz litery która zaczyna nazwę danego elementu.

#### Sterowanie w oknie wyboru certyfikatów

	Wybier	rz certyfikat		
ta certyfikatów				
Wystawiony dla:	Wydany przez:	Termin ważności:	Numer	seryjny:
mikolaj.narowski@enigma.com.		25/05/2023 14:24:31	80	
zczegóły certyfikatu				
Numer seryjny :				80
Wystawiony dla:				
SURNAME=Narowski, GIVENNAME=Mikołaj, Cl	N=mikolaj.narowski@enigma.cor	n.pl, C=PL		
Wydany przez:				
CN= C=PL				
Termin ważności:		2	5/05/2021 14:24:31 - 25/0	5/2023 14:24:31
			n	ezaprzeczalność
Użycie klucza:				capizedaniose
Użycie klucza:				

Poruszanie się klawiaturą w tym oknie ma dwojaki charakter, w zależności od aktualnie wybranego komponentu:

- Po każdym głównym elemencie (komponent tabeli, pola tekstowe oraz jego suwaki, przyciski) można przechodzić klawiszem Tab.

- Po wylistowanych certyfikatach w komponencie tabeli można przechodzić strzałkami w górę oraz w dół.

Aby wybrać certyfikat, oznaczony kolorem czerwonym, należy nacisnąć Enter lub Spację. Wybór certyfikatu jest sygnalizowany oznaczeniem check-box'a po lewej stronie wiersza tabeli.

## B.5 Współpraca z usługą mobilnego podpisu elektronicznego

Aplikacja CertSign może współpracować z mobilną usługą podpisu elektronicznego, o ile dostawca zapewnia oprogramowanie do emulacji obsługi karty kryptograficznej, umożliwiające rejestrację certyfikatów w magazynie certyfikatów Windows (CSP) lub dostęp przez sterownik PKCS#11. Przygotowanie CertSign do współpracy polega na wyborze certyfikatu dostarczonego w ramach usługi mobilnej w konfiguracji CSP (magazyn Windows) lub PKCS#11. Pozostałe kroki przebiegają jak dla zwykłego podpisu, z uwzględnieniem autoryzacji w aplikacji mobilnej. Poniżej opisano przykładowo współpracę z usługą mSzafir. W podobny sposób można uzyskać współpracę z inną usługą, np. SimplySign <a href="https://pomoc.certum.pl/pl/simplysign-faq/">https://pomoc.certum.pl/pl/simplysign-faq/</a>

![](_page_44_Picture_0.jpeg)

W celu przygotowania mSzafir należy postępować zgodnie z instrukcją:

https://www.mszafir.pl/gfx/mszafir/userfiles/\_public/tutoriale/jak\_wykorzystac\_certyfikat\_mszafir\_w\_dowolnej \_aplikacji\_podpisujacej.pdf

Po aktywowaniu karty wirtualnej należy w CertSign wybrać opcję "Zmień certyfikat" i wskazać certyfikat usługi mobilnej, analogicznie jak w przypadku zwykłego certyfikatu (w konfiguracji CSP lub PKCS#11).

Wystawiony dla:         Wydany przez:         Termin ważności:         Numer seryjny:           Image: State of the state of	277
COPE SZAFIR - Kwalifikowany         14/04/2023 11:56:26         55710f80432f4b7e0532 6bf02f97220aad482           Material Science         CCK MF Zewnetrzne         04/02/2024 15:30:54         23cf6           Material Science         CCK MF Zewnetrzne         19/10/2022 13:09:33         1e199           Material Science         TEST CCK MF Zewnetrzne         18/11/2023 08:58:16         27ff           zczegóły certyfikatu         Science         27ff         27ff	277
Image: Second state         CCK MF Zewnetrzne         04/02/2024 15:30:54         23cf6           Image: Second state         CCK MF Zewnetrzne         19/10/2022 13:09:33         1e199           Image: Second state         TEST CCK MF Zewnetrzne         18/11/2023 08:58:16         27ff	_
Line         CCK MF Zewnetrzne         19/10/2022 13:09:33         1e199           Image: State St	
TEST CCK MF Zewnetrzne 18/11/2023 08:58:16 27ff	
czegóły certyfikatu	
Wydany przez:	
Wydany przez: OID.2.5.4.97=VATPL-5260300517, CN=COPE SZAFIR - Kwalifikowany	^
Wydany przez: OID.2.5.4.97=V ATPL-5260300517, CN=COPE SZAFIR - Kwalifikowany O=Krajowa Izba Rozliczeniowa S.A., C=PL	$\hat{\mathbf{v}}$
Wydany przez:           OID.2.5.4.97=VATPL-5260300517, CN=COPE SZAFIR - Kwalifikowany           O=Krajowa Izba Rozliczeniowa S.A., C=PL           Termin ważności:         14/04/2022 11:56:27 - 14/04/2023 11:	<b>\$</b> 56:26

Po wybraniu certyfikatu można przejść do podpisania dokumentu, przy czym autoryzacji podpisu dokonuje się podając kod wygenerowany w aplikacji mobilnej.

![](_page_44_Picture_6.jpeg)

#### Potwierdzenie

Porównaj skrót dokumentu prezentowany powyżej z wyświetlonym na ekranie i jeżeli jest zgodny potwierdź operację podpisania na telefonie.

#### Status podpisywania

Przetwarzanie

![](_page_45_Picture_0.jpeg)

## B.6 Szczególne przypadki dotyczące kart z certyfikatami kwalifikowanymi

W przypadku podpisu kwalifikowanego CertSign do komunikacji z kartą kryptograficzną wykorzystuje usługi CSP lub PKCS#11. W niektórych przypadkach może się jednak okazać, że specyfika interfejsów karty kryptograficznej i CertSign wymusza użycie tylko jednej z w/w usług.

# UWAGA! Należy zainstalować również oprogramowanie dostawcy certyfikatu kwalifikowanego, gdyż zawiera ono sterowniki do kart kryptograficznych.

Jeśli podczas podpisywania z wybraną opcją CSP wystąpi błąd, np.:

![](_page_45_Picture_5.jpeg)

W czasie podpisywania dokumentu wystąpił wyjątek. Prawdopodobny powód błędu: Exception raised in JCAPI.DLL: JCAPISignature\_sign() - Could not acquire a key container handle for CSP: cryptoCertum3 CSP Kod błędu: E\_ERROR\_SIGNING\_WITH\_PRIVATE\_KEY

należy w CertSign wybrać opcję *Zmień certyfikat*, wskazać *PKCS#11* oraz ścieżkę do pliku .dll sterownika karty, dostarczonego z oprogramowaniem dostawcy certyfikatu. Należy przy tym zwrócić uwagę na wybór pliku odpowiedniego dla architektury systemu operacyjnego (32 lub 64 bitowej).

Informacji o lokalizacji tych plików należy poszukiwać na stronach lub w dokumentacji dostawcy certyfikatu. W przypadku polskich dostawców **mogą** to być:

### CERTUM:

C:\Windows\System32\cryptoCertum3PKCS64.dll

C:\Windows\System32\cryptoCertum3PKCS.dll

https://pomoc.certum.pl/pl/ekw-reczne-wskazanie-sterownika-karty-kryptograficznej/

### SIGILLUM:

C:\Windows\System32\asepkcs.dll

### EUROCERT:

C:\Windows\System32\cmP11.dll

C:\Windows\System32\cmP1164.dll

C:\Windows\SysWOW64\cmP11.dll

https://eurocert.freshdesk.com/support/solutions/articles/48001213718-niezb%C4%99dna-bibliotekalocalizacja-

### KIR (Szafir):

C:\Program Files\Krajowa Izba Rozliczeniowa S.A.\Szafir 2.0\bin\CCGraphiteP11p.x64.dll C:\Program Files\Krajowa Izba Rozliczeniowa S.A.\Szafir 2.0\bin\CCGraphiteP11p.x86.dll https://www.elektronicznypodpis.pl/gfx/elektronicznypodpis/userfiles/ public/informacje/instrukcje/instrukcja

konfiguracji\_kart\_cryptocard\_graphite\_w\_jpk.pdf

C:\Program Files\CryptoTech\CCP1164.dll

C:\Program Files\CryptoTech\CCPkiP11.dll

https://www.elektronicznypodpis.pl/gfx/elektronicznypodpis/userfiles/\_public/informacje/instrukcje/jpk\_2.pdf CENCERT:

C:\Program Files\ENCARD\enigmap11-x64.dll C:\Program Files (x86)\ENCARD\enigmap11.dll

Szczególnym przypadkiem są karty kryptograficzne zabezpieczane na 2 poziomach: kodem PIN do karty oraz odrębnym PIN-em do wykonania podpisu. Przykładem może być karta IDPrime dostarczana przez CenCert (biała z niebieskim logo), która posiada PIN do karty oraz *Digital Signature PIN* do wykonania podpisu. Proces podpisania w CertSign wymaga wówczas podania kolejno obu PIN-ów i jest to dostępne **jedynie w konfiguracji CSP**. Użycie PKCS#11 spowoduje, że przekazywany będzie tylko PIN karty i podpis nie zostanie wykonany.

![](_page_46_Picture_0.jpeg)

Poniżej pokazano dla przykładu, jak wykonać podpis z użyciem karty IDPrime od CenCert (wymaga ona zainstalowanego oprogramowania *SafeNet Authentication Client*).

Przy wybranej konfiguracji CSP i certyfikacie kwalifikowanym (zakładka *Certyfikaty/Log*) należy wskazać plik do podpisania i zatwierdzić podpisanie. W pierwszym kroku pojawi się pytanie o PIN do karty kryptograficznej.

Certyfikaty/Log	🙋 Podpis				
Pliki					
	C:\Useshellowhite	tooloonob14.20 ml		~	
Pliki do podpisu		ur private key has be ease enter PIN code fr	en requested for signing. or Card #29A7156B4C0011	19:	
Folder docelowy	С: /Users исклатиреем	Ok	Cancel		
Parametry podpisu			1		
Format podpisu	XadES	CadES OPadES	Podpisywanie dai	nych	
Algorytm skrótu	SHA256	O SHA512			

Po podaniu prawidłowego PIN-u karty wyświetlone zostanie żądanie Digital Signature PIN.

	C:\Use	🤶 Digital Signature PIN Log	on	×
Pliki do podpisu		SafeNet Authentic	ation Client	THALES
		Enter the Digital Signature PIN:		
Folder docelowy	C:\Us	Nazwa tokena:	Card #29A7156B4C00	1119
		Digital Signature PIN:	•••••	
rametry podpisu			Bieżący język: Pl	-
Format podpisu				

Wykonanie podpisu zostanie potwierdzone komunikatem.