



Oprogramowanie do podpisu elektronicznego i zarządzania kartami kryptograficznymi,

dostarczane przez centra certyfikacji

- ustawienia dla Systemu e-Deklaracje

Informacja o centrach certyfikacji Ι.

Rejestr kwalifikowanych podmiotów świadczących usługi certyfikacyjne jest opublikowany przez Narodowe Centrum Certyfikacji (NCCert) na stronie <u>www.nccert.pl</u>

Oferowane w zestawach do podpisu oprogramowanie:

- 1. Kwalifikowane Centrum Certyfikacji Kluczy CenCert (www.cencert.pl)- "PEM-HEART Signature" wersja 3.9.12.37 - składanie podpisu i zarządzanie kartami (https://www.cencert.pl/Oprogramowanie%20PEMHEART/)
- 2. Centrum Obsługi Podpisu Elektronicznego Krajowej Izby Rozliczeniowej S.A. (www.elektronicznypodpis.pl)- "SZAFIR" wersja 2.0.0 build 590 - składanie podpisu, "CryptoCard Suite" wersja 2.1.170 – zarządzanie kartami (http://www.elektronicznypodpis.pl/informacie/aplikacie/)
- 3. Centrum Usług Zaufania Sigillum (<u>www.sigillum.pl)-</u> "PWPW Sign" 5.2.3 – składanie podpisu, "CryptoCard Suite" wersja 2.1.170 – zarządzanie kartami

(http://sigillum.pl/pliki_do_pobrania.html)

- 4. Powszechne Centrum Certyfikacji CERTUM (<u>www.certum.pl</u>) "proCertum SmartSign + SimplySign Desktop" wersja 8.1.16.1 build 2725 - składanie podpisu, "proCertum CardManager" wersja 3.2.0.156 - zarządzanie kartami (https://certum.pl/certum/cert,oferta_oprogramowanie_biblioteki.xml)
- 5. Centrum Certyfikacji EuroCert (<u>www.eurocert.pl</u>) "EuroCert SecureDoc" wersja 2.0 - składanie podpisu, "Charismathics Smart Security Interface Standard" zarządzanie kartami wersja 5.0.3, 5.2.2 i 5.4.3

https://eurocert.pl/index.php/oprogramowanie

https://eurocert.pl/pub/Oprogramowanie/eurocert_oprogramowanie.exe https://eurocert.pl/pub/Oprogramowanie/SecureDoc/SecureDoc 2 setup.exe

Dokument uwzglednia:

* - stan na dzień 12.09.2018 r.

** - Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2016 poz.1579)

Art. 137. Do dnia 1 lipca 2018 r. do składania zaawansowanych podpisów elektronicznych lub zaawansowanych pieczęci elektronicznych można stosować funkcję skrótu SHA-1, chyba że wymagania techniczne wynikające z aktów wykonawczych wydanych na podstawie rozporządzenia 910/2014 wyłączą możliwość stosowania tej funkcji skrótu





CryptoCard komponen Suite tu 2.1.170 technicz...



Podpis proCertum Elektronicz CardMana ny PWPW ger 3.2.0.156 SIGN 5.2.3



(build 272







Interface

Szafir 2.0.0 ((build 590)









II. Ustawienia oprogramowania

- 1. CenCert "PEM-HEART Signature"
 - a. instalacja certyfikatu w systemie





b. konfiguracja formatu podpisu

W









Į	PEM-HEAR	T Signatur	e							_		×
	🔏 Usta	wienia										
F	odpisywanie	Pliki	Proxy	PIN	Certyfikaty	Listy TSL	Ogólne	Aktualizacje	Import danych			
1	Format i typ	p podpisu										^
	Rozszerz	zenie		Ор	cje rozszerze	nia						
	* *			F	ormat podpisu							
	*.PDF				• XAdES (no	rma ETSI TS	101 903)					
	*.XML											
					XAdES of	aczający						
					XAdES of	oczony (tylk	u o dla plików	XMI.)				
					CAdES, CN	1S (norma E	TSI TS 101	733)				
					CAdES, C	CMS w osobn	ym pliku					
					O CAdES, S/	MIME (norma	ETSI TS 10	1 733)				
					O PAdES (ty	lko dla plików	PDF) (norr	na ETSI TS 102	778)			
			•		O ASiC (norm	a ETSI TS 10)2 918)					
	🗌 Dodaj zr	nacznik czas	su									
	Dodaj od	dpowiedź O	CSP									
	Zakoduj	base64 dol	kumenty xr	nl podcza:	s składania podp	oisu otaczają	cego XAdES					
	Dodaj ro	odzaj zobow	liązania	potwier	dzenie pochodz	enia (proof o	f origin)	Ψ.				
	Algorytmy	kryptogra	ficzne									_
	Algorytm	skrótu			SHA-256	•						~
										Zapisz	An	uluj









2. KIR S.A.

a. "CryptoCard Suite" - instalacja certyfikatu w systemie operacyjnym – kolejne kroki

Ogólne	Karty elektroniczne	Narzędzia	Konfiguracja		
- Asyste	Pozwala skontri oprogramowani	olować czy w a CryptoCard	vszystkie składnik Suite funkcjonują	i systemu operac poprawnie.	syjnego i
Mena	dżer certyfikatów Służy do zarząc	Izania certyfi	katami w systemie	operacyjnym.	JChom
Dodat	kowe narzędzia			Un	uchom
and the second se	Pozwalają na st otrzymanego ce operacyjnym.	worzenie wn rtyfikatu na k	iosku o certyfikat carcie elektroniczr	oraz zainstalowa nej i w systemie	nie
			6	Dr.	uchom

🥁 CryptoCard Suite: Dodatkowe narzędzia	×
Wybór asystenta Wybierz rodzaj asystenta, który ma być uruchomiony.	Szafy
 Wniosek o certyfikację Wniosek o recertyfikację Importu certyfikatu lub klucza prywatnego Rejestracja certyfikatu w systemie 	
Informacja o asystencie: Ten asystent pozwala Ci zarejestrować w systemie operacyjnym certyfikat znajdujący się na karcie elektronicznej. Jest to potrzebne dla aplikacji takich jak Outlook, Outlook Express, Internet Explorer.	-
< Wstecz Dalej > Anuluj Pomoc	;









🍯 CryptoCard Suite: Dodatkowe narzędzia	×
Wybierz dostępną kartę elektroniczną	KIR. Szafy
Wybierz kartę elektroniczną	
Broadcom Corp Contacted SmartCard 0 KI Token 1 KI Token 2 KI Token 3 QESv2 Broadcom Corp Contactless SmartCard 0	
< Wstecz Dalej > Anuluj	Pomoc

<u>(</u>	CryptoCard S	Suite: Dodatkowe narzędzia		×						
h	Import certyfikatu Ten asystent pozwala ci zarejestrować certyfikat X.509 w systemie operacyjnym.									
۷	Wybrany certyfikat:									
	Wydany dla	Wydany przez	Ważny od	Ważny do						
		COPE SZAFIR - Kwalifikowany	2016.03.22. 7:30.00	2018.03.22. 7:30						
	/									
L	`			~						
			Zaloguj	Więcej						
		< Wstecz Dale	ej > Anuluj	Pomoc						







CryptoCard Suite: Dodatkowe narzędzia X								
Wniosek o recertyfikację Ten asystent pozwala ci zarejestrować certyfikat X.509 w systemie operacyjnym.								
Zarejestruj certyfikat w systemie operacyjnym								
Przyjazna nazwa:	Nazwa podana przez użytkownika							
Magazyn certyfikatów:	Osobisty	~						
Moduł CSP	Crypto Tech CSP	~						
<	Wstecz Zakończ Anuluj	Pomoc						

b. "SZAFIR" - konfiguracja formatu podpisu











🗑 Szafir 2.0.0 (build 590)			×
Plik Narzędzia Okno Pomoc			
Dostępne konfiguracje		×	
🔿 <konfiguracja domyślna=""> [aktywna]</konfiguracja>	Dodaj		
	Usuń		
	Zmień		
		4	11
	Opcje		
		_ 1	
Pomoc Zastosuj	Anuluj		
KIR- Szafir znakowy w zakrzego z polokowy z concernencie prawa autorskie stanowią w samo w szelkie prawa zastrzeżone. Licencjonowanie odbywa sie na zasadach ustalonych przy znaklem towarowym. Powyższe oprogramowanie obejmuje także dokumentacje użytk	ez KiR S.A. Szafir jest zasi ownika oraz wszelkie inr	trzeżonym ne dokumenty	i
związane z miniejszym oprogramowaniem.			

Konfigur	acja								×
Nazwa	<konfiguracja domyślna=""></konfiguracja>								
	składanie podpisu 🛛 V	, O veryfikacja	C) znakowanie czasem	ि szyfrowanie	komp tech	の の niczny	Ustawienia sieciowe	eArchiwum	
	Certyfikat dla podpisu Dowolny certyfikat v Wybierz								
Para	Parametry podpisu Polityka Źródła / wyniki podpisu Format: O CAdES (PKCS#7) Dodaj kolejny podpis do pliku z podpisem © XAdES Parametry podpisu Wariant: Nie dołączaj dodatkowych informacji (XAdES-BES) Dodaj kolejny podpis do pliku z podpisem © XAdES PAdES /dla plików PDF/ Funkcja skrótu: SHA-256 Zapisz podpisywane dane razem z podpisem Rodzaj zobowiązania: Brak zobowiązań Nie koduj danych XML'owych do Base64 Podpis wbudowany (kontrasygnata) Podpis otaczany Podpis zgodny z eDeklaracje								
Pom	Pomoc Przywróć ustawienia fabryczne Zapisz Anuluj								









3. Sigillum

- a. "**CryptoCard Suite**" instalacja certyfikatu w systemie operacyjnym identycznie jak w pkt 2.a
- b. "Sigillum Sign 4" konfiguracja formatu podpisu

Sgi Lum Sign 4 Operacje Konfiguracja Pomoc		
tawienia Certyfikaty Serwery	S Ustawienia podpisu 🕑 🔀	
Opcje programu tus pliku Plik	Domyślny format podpisu	
	Profi podpisu Dla systemu E-Deklaracje 💌 🔶 A	adres 🙀 Komputer 💽 🔇 🛇 🖉
	Domyślny format podpisu	Nazwa Rozmiar Typ Zmo.,
	XAdes CMS CAdes PAdes	C:\ Folder 2013
	Ustawienia typu podpisu	
	Typ podpisu: Otaczający 🕬	
	Wariant podpisu AdES: BES (M)	
	Funkcja skrótu: SHA-1 👒	
	Typ zobowiązania: Brak imi	
	💓 Nie koduj podpisanych danych XML algorytmem base64	
	Plik wynkowy	
	sposoo zapisu: Wszystkie podpisy w jednym pliku 💌	
Tabela jest pusta	Aby Domyśliny klient poczty: Microsoft Outlook	
	Obsługiwane polityki Polityki podpisu Polityki podpisu	
	Przywróć ustawienia domyśne OK Anuluj	









c. "**PWPW Sign 5**" - konfiguracja formatu podpisu

PWPW Sign 5					-	
PWPW	Sign 5				P	
			V			
Podpisz	Doda podp	nj kolejny Dis	Weryfikuj			
	A			G	Ð	
Szyfruj	Zaaw	vansowane	Odszyfruj	C	ertyfikaty	
Zmiana widoku					Pomoc	Ustawienia
PWPW Sign 5					_	
🗲 Ustawie	enia apli	kacji			P	
 Czas lokalny Serwer czasu NTP 			Proxy delin, auto Autoryzacja pod	czas st		
Ustawienia	РКІ					
Domyślny profil	Profil podpisu	Domyślny alg	orytm Polityki ce	ertyfikacji		
Profil podpisu	Użytkownika		•	Nowy	Usuŕ	,
Nazwa profilu	e-Deklaracje SHA2					
Format	XAdES +	Wariant	BES (nie zaw *	Тур	Otaczający	
Typ zobowiązania	Brak +	Funkcja skrótu	SHA-256 •	Domyślny	Tak	
		Ual Ustaw jal	ktualnij ko domyślny			
						v
Zapisz Ustawienia domy	rślne					Pomoc









4. **CERTUM**

a. "proCertum CardManager" - instalacja certyfikatu w systemie operacyjnym

🖾 proCertum CardManager										
proCe	rtum CardManager									
Nazwa czytnika: Broadcom Corp Contacted SmartCard 0	Zamknij <u>k</u> artę									
Informacja o karcie 🔟 Profil bezpieczny 🔞 Profil zwykły 🔒 Profil UniLock										
PIN i PUK	Zmień PI <u>N</u>									
Status kodu PIN: OK	Nowy PIN									
Status kodu PUK: OK	Zmi <u>e</u> ń PUK									
Lista certyfikatów	Zapisz certyfikat									
Właściciel certyfikatu Wystawca certyfikatu	Data ważności									
CERTUM QCA										
Pok <u>a</u> ź szczegóły certyfikatu	<u>R</u> ejestruj certyfikaty									
Opgie	<u>O</u> programie <u>Z</u> akończ									

b. "proCertum SmartSign" - konfiguracja formatu podpisu

🕲 proCertum Si	martSign - Ustawier	iia	- X	N		_ 🗆 X
Podpisywanie	W eryfikowanie	Ç Ust <u>a</u> wienia	O Po <u>m</u> oc	i <u>O</u> programie		
Ogólne	Podpis	Weryfikacja	Znacznik czasu			
 Format podplsu XAdES Podpis XAdES - Pelektronicznym. F CAdES/ETSI Podpis CAdES/ETSI Podpis CAdES/ETSI Podpis zewnęt Plik podpisu będ podpisem. Podpis wewnęt 	Podpis elektroniczny w f Format zgodny z najnov FSI - Podpis elektroniczn Starszy format podpisu e rzny zie zawierał tylko inform	ormacie XAdES jest zg vszymi standardami oj y w formacie CAdES/E elektronicznego. acje o podpisie. Pami	odny z wymaganiami Us barty o język XML i zaleca TSI jest zgodny z wymag ętaj jednak, że w trakcie s	stawy z dnia 18 września any do powszechnego st ganiami Ustawy z dnia 18 weryfikacji podpisu trzeb	2001 roku o podpisie osowania. września 2001 roku o podp a dostarczyć dokument wra:	nisie zz
Funkcja skrótu	zie rownież zawierał tres	с аокитепtu. А-256 🔻				
Ustawienia	domyślne					
inisterstwo	MINISTER	STWO FINANS ul. Świętokrz www.mf.gov e-mail: i	ÓW DEPARTAN zyska 12, 00-916 v.pl www.e-Deklara nfo.e-deklaracje@mf	IENT INFORMAT Warszawa acje.gov.pl .gov.pl	YZACJI	Administra







Archiwlzacja Kopiuj po podpisaniu Po wygenerowaniu podpisu zostanie on skopiowany do wybranego katalogu wraz z podpisanym dokumentem, jeśli wygenerow zewnętrzny. Image: Comparison of the state of t	vano podpis Wybierz
Domyślny certyfikat Informacje: Podmiot: Wystawca: Numer seryjny:	Wybierz Pokaż Usuń
Dodatkowe opcje podpisu Przed podpisem pytaj o powód podpisu Image: Twórz podpis specjalny PDF (PAdES), gdy podpisywany jest dokument PDF	
 Sprawdzaj ważność certyfikatu online przed rozpoczęciem podpisywania Wyłącz obsługę czytników kart z wbudowaną klawiaturą (PINPAD) oraz klawiatur z wbudowanymi czytnikami kart Wybierz rodzaj zobowiązania: Formalne zatwierdzenie (Proof of approval) 	
Wafarit podpisu: Nie dorączaj dodatkowych informacji (bes) Opcje konfiguracji znacznika czasu znajdują się w panelu: Znacznik czasu Zaawansowane opcje podpisu ETSI/CAdES Scieżka do pliku polityki podpisu:	
Informacje o polityce podpisu: Zaawansowane opcje podpisu PDF/PAdES Scieżka do pliku polityki podpisu:	
Informacje o polityce podpisu:	
Plik symbolu: Lokalizacja podpisującego:	
Twórz podpis dołączony (Enveloped), gdy podpisywany jest dokument XML podpisem wewnętrznym XAdES Twórz podpis dołączony (Enveloped) w wersji standardowej	







c. **SimplySign Desktop** (dostępnej z paska zadań, *po kliknięciu prawym klawiszem myszki*) Konfiguracja aplikacji

🛃 SimplySign Desktop	Х
Орсје	
└── Uruchamiaj przy starcie systemu	
Pamiętaj identyfikator ostatniego użytkownika	
🗹 Pokazuj okienko logowania gdy aplikacja zażąda dostępu do SimplySign	
🗌 Pokazuj okienko logowania przy uruchamianiu SimplySign Desktop	
Wyrejestruj certyfikaty po odłączeniu od SimplySign	
Pamiętaj kod PIN dla aplikacji korzystających z CSP/KSP	
Zapomnij kod PIN po odłączeniu od SimplySign	
Język: Polski 🗸	
Ok Anuluj	

Logowanie do aplikacji SimplySign Desktop

Projekt

e-Deklaracje2



Lista dostępnych certyfikatów w aplikacji (*przykład poniżej pokazuje listę obejmującą 2 certyfikaty, standardowo użytkownik na liście będzie miał 1 certyfikat*)

Medicial.		
właściciel. Numer seryjny certyfikatu: Wystawca: Okres ważności certyfikatu: Klucz publiczny: Numer karty:	kwalitikowany 0F AF 25 E6 71 31 6D 07 4F AD 85 4F 32 45 Certum QCA 2017 23.03.2018 - 22.03.2020 RSA, 2048 bitów 7649 6170	
Właściciel: Typ certyfikatu: Numer seryjny certyfikatu: Wystawca: Dkres ważności certyfikatu: Rlucz publiczny: Numer karty:	kwalifikowany 1A 90 85 C2 F1 B1 29 E3 E2 77 6A EB 6F F4 CERTUM QCA 23.03.2018 - 22.03.2020 RSA, 2048 bitów 7785 3774 0890 2315 [CertSHA1]	









5. EuroCert SecureDoc

a. "**Charismathics Smart Security Interface**" - instalacja certyfikatu w systemie operacyjnym



b. "EuroCert SecureDoc" - konfiguracja formatu podpisu

SecureDoc							- 0	×
Podpi	Wariant podpisu: Typ podpisu: Funkcja skrótu:	kowanie Ustawienia XAdES-BES (nie zawiera znacznika czasu) v Wewnętrzny v SHA-256 v	🗌 Dodaj kolejny podpis	Dodaj Usu plik plik	ń Dodaj katalog	Wyczyść listę	Pokaż dokument	Podpisz pliki
Format podpisu		Parametry podpisu				Dane		
Dane wejściowe (0)		Dane wyjściowe (0)			Status			



