INSTRUKCJA UŻYTKOWNIKA

Użycie kwalifikowanego podpisu elektronicznego zapisanego na karcie kryptograficznej w programie Adobe Reader (system Windows)

Wersja 1.0

Spis treści

1.	١	Wstęp	3			
2.	١	Wymagania sprzętowo-programowe	3			
3.	ι	Użycie kwalifikowanego podpisu elektronicznego				
	3.1	. Wyłączenie trybu bezpiecznego	3			
	3.2	. Dodanie do konfiguracji sterownika czytnika kart	4			
	3.3	. Wykonanie podpisu	5			

1. Wstęp

Niniejsza instrukcja przedstawia proces konfiguracji oprogramowania Adobe Reader do współpracy z kwalifikowanym podpisem elektronicznym Certum zapisanego na karcie kryptograficznej.

2. Wymagania sprzętowo-programowe

Do poprawnego współdziałania certyfikatów Certum z aplikacją Adobe Reader konieczne jest spełnienie poniższych wymagań sprzętowo-programowych:

- Zainstalowane oprogramowanie proCertum CardManager
- Zainstalowany czytnik kart
- 3. Użycie kwalifikowanego podpisu elektronicznego

3.1. Wyłączenie trybu bezpiecznego

Aby możliwe było podpisywanie w Adobe Reader trzeba wyłączyć tzw. tryb chroniony. W tym celu, z Menu aplikacji należy wybrać **Edycja → Preferencje → Zabezpieczenia** (rozszerzone) i wyłączyć opcję **Podczas uruchamiania włącz tryb chroniony**. Po wyłączeniu trybu chronionego należy zrestartować aplikację.

	Exception protection protections	
menty intowanie	Podczas uruchamiania włącz tryb chroniony 🖉 Uruchom w AppContainer 🔹 Utwórz plik dziennika trybu chronioneg	• Wyświetł dziennik
ne	Podgląd chroniony Wyk.	
ekran	Pliki z potencjalnie niebezpiecznych lokalizacji	
ietlanie strony	O Wszystkie pliki	
wartość multimedialna		
ie	Rozszerzone zabezpieczenia	
nosc	✓ Włącz rozszerzone zabezpieczenia	niędzy domenami <u>Wido</u>
iarze +		
rint .	Położenia uprzywilejowane	
tki	lefii urtaviania zabeznieczeń maja perstavny wokay na Twój obieg pracy, utyć Lokalizacji	
	uprzywiej osawielia zabecpieczenia mają negacywi y wpisy na woj osreg pracy, czy jeckalizacji uprzywiej osawielia zabecpieczenia nadawać status zaufanych plikom, folderom i hostom w	
e-mail	celu ominiecia ograniczeń. Lokalizacje uprzywilejowane zapewniają bezpieczeństwo pracy	
lżer zaufania	oraz pozwalają nadawać status zaufanych elementom obiegu pracy.	
śledzący	Automatycznie ufaj dokumentom z ważnym certyfikatem	
iedia (starsze)		
У	Zobacz zaufane witryny systemu Windows Zobacz zaufane witryny systemu Windows	
10 1		
r (Geo)		
r (Geo) zowanie		
r (Geo) zowanie dzanie pisowni		
r (Geo) zowanie dzanie pisowni ność Adobe Online		
r (Geo) cowanie dzanie pisowni ność Adobe Online urowanie (2D)		
r (Geo) cowanie dzanie pisowni ność Adobe Online irrowanie (2D) irrowanie (3D)		
r (Geo) cowanie zanie pisowni ność Adobe Online nrowanie (2D) prowanie (3D) kiwanie		
r (Geo) zowanie dzanie pisowni mość Adobe Online arowanie (2D) arowanie (3D) kiwanie <u>jieczenia (rozszerzone)</u>		
r (Geo) zowanie dzanie pisowni mość Adobe Online arowanie (2D) arowanie (3D) kiwanie pieczenia (rozszerzone)		
r (ueo) isowanie Izanie pisowni ność Adobe Online irowanie (2D) rowanie (3D) kiwanie ieczenie (rozszerzone) ieczenie ie do multimediów (starsze		
r (ueo) dzanie pisowni ność Adobe Online trowanie (2D) trowanie (3D) kiwanie nieczenia (rozzzerzone) nieczenia sie do multimediów (starsze		
r (ueo) dzanie pisowni mość Adobe Online Adobe Online arowanie (2D) srowanie (3D) kiwanie pieczenie (rozzerzone) pieczenie nie do multimediów (starsze		
r (ueo) cowanie dzanie pisowni ność Adobe Online Arowanie (2D) srowanie (SD) srowanie		
r (ueo) dzanie pisowni ność Adobe Online rowanie (2D) rowanie (3D) kiwanie <u>pieczenie</u> ie do multimediów (starsze	e) Dodaj plik Dodaj ścieżkę folderu Dodaj hosta	Usuň
(teo) tzanie pisowni tość Adobe Online rowanie (2D) rowanie (3D) tiwanie (eczenie (rozzzersone) ieczenie ie do multimediów (starsze	e) Dodaj plik Dodaj ścieżkę folderu Dodaj hosta	Usuń
(ueo) owanie tzanie pisowni ość Adobe Online (zowanie (2D) rowanie (3D) rowanie (3D) riwanie (ieczenia (rozerzone) ieczenie ie do multimediów (starsze	e) Dodaj plik Dodaj ścieżkę folderu Dodaj hosta <u>Co to jest Podplad chroniony?</u> <u>Czym sa Rozszerzone zabezpieczenia?</u> <u>Czym sa Lokalizacje uprzywilejowane?</u>	Usuň

Rysunek 1 – Wyłączenie trybu chronionego

3.2. Dodanie do konfiguracji sterownika czytnika kart

W celu umożliwienia złożenia podpisu certyfikatem zawartym na karcie kryptograficznej należy najpierw w opcjach dodać sterownik czytnika kart kryptograficznych. W tym celu należy wybrać z Menu **Edycja → Preferencje → Podpisy**.

ferencje		
ategorie:		
Dekumentu	Podpisy elektroniczne	
Comentowanie	Tworzenie i wygląd	
adine		
Debug ekran	 Opcje sterowania związane z tworzeniem podpisów 	Wiecei
Vyświetlanie strony	 Ustal wygląd podpisów w dokumencie 	
D i zawartość multimedialna	Weryfikacja	
zytanie		
Jostępność	 Kontroluj w jaki sposób i kiedy podpisy są weryfikowane 	Wiecej
ormularze		
nternet		
avaScript	Tożsamości i certyfikaty zaufane	
ednostki		N
zyk	 Tworzenie i zarządzanie tożsamościami na potrzeby podpisywania 	Wiecei
onta e-mail	 Zarządzanie poświadczeniami używanymi do nadawania dokumentom statusu zaufanych 	
Aenedżer zaufania		
Aoduł śledzący	Dodawanie znaczników czasowych do dokumentów	
Aultimedia (starsze)	· · · · · · · · · · · · · · · · · · ·	
odpisy	 Konfiguracja ustawień serwera znaczników czasowych 	Wiecei
omiar (Geo)		
ecenzowanie		
prawdzanie pisowni		
ożsamość		
Jsługi Adobe Online		
Vymiarowanie (2D)		
Vymiarowanie (3D)		
Vyszukiwanie		
abezpieczenia (rozszerzone)		
abezpieczenie		
aufanie do multimediów (starsze)		
		OK Anuluj

Rysunek 2- Opcje - sekcja Podpisy

W sekcji Podpisy, z sekcji Tożsamości i certyfikaty zaufane należy wybrać przycisk Więcej.

W kolejnym kroku należy rozwinąć menu **Elektroniczne ID** i wybrać **Moduły i znaczniki PKCS#11,** następnie nacisnąć przycisk **Dołącz moduł**.

í	🔒 Ustawienia identyfikatora cyfroweg	go oraz zaufanego certyfikatu				×
\sim	/ Elektroniczne ID	Dołącz moduł	Odłącz moduł	C Odśwież		
	Konta ID roamingu	ID twórcy modułu	Ścieżka bibli	oteki		
	Pliki Elektroniczne ID					
	Identyfikatory elektroniczr	1				
	Moduły i znaczniki PKCS#	$\langle \neg$				
	Zaufane certyfikaty)	
		Zarządzaj modu	ułami PKCS#11			
		Lista wczytanych m nowych urządzeń k	aodułów PKCS#11. D ryptograficznych	odatkowe moduły n	nogą zostać wczytane w celu uzyskania dos	tępu do

Rysunek 3 – Opcje – Moduły PKCS#11

Należy wskazać plik C:\WINDOWS\system32\cryptoCertum3PKCS.dll i nacisnąć przycisk **Otwórz**. Po zainstalowaniu sterownika czytnika kart należy zrestartować aplikację.

3.3. Wykonanie podpisu

W celu wykonania podpisu należy na pasku menu wybrać kolejno **Plik > Otwórz**. Następnie wyszukać dokument do podpisania w formacie PDF i kliknąć **Otwórz**.

Po wybraniu dokumentu należy przejść do sekcji Narzędzia > Certyfikaty > Podpisz cyfrowo.



Rysunek 4 – Certyfikaty – Sekcja Narzędzia



Rysunek 5 – Podpisanie cyfrowe dokumentu

W kolejnych krokach należy:

- Wybrać miejsce złożenia podpisu
- Wybrać swój certyfikat kwalifikowany
- Zapisać plik
- Podać kod PIN do e-podpisu.