Certum Code Signing

Instrukcja certyfikatu Code Signing SimplySign

Wersja 1.0

Certum

Spis treści

1.	Ws	stęp		3					
2.	Wy	Wymagania formalne do wydania certyfikatu Code Signing3							
3.	Ak	Aktywacja certyfikatu Code Signing SimplySign w Sklepie CERTUM							
4.	Uz	yskai	nie dostępu do certyfikatu po jego wydaniu	12					
5.	Po	dpisy	/wanie w środowisku Windows	16					
	5.1.	Spr	rawdzenie dostępu do usługi i wyświetlenie certyfikatów	16					
	5.2.	Poo	dpisywanie narzędziem signtool	21					
	5.2	2.1.	Podpis pojedynczy	21					
	5.2	2.2.	Podpisywanie wsadowe	23					
	5.2	2.3.	Podpis dualny	23					
	5.3.	We	eryfikacja podpisu narzędziem signtool	24					
	5.4.	Poo	dpisywanie narzędziem jarsigner	25					
	5.4	1.4.	Utworzenie pliku konfiguracyjnego provider.cfg	25					
	5.4	1.5.	Utworzenie pliku ścieżki certyfikatu bundle.pem	26					
	5.4	1.6.	Uzyskanie aliasu certyfikatu	32					
	5.4	4.7.	Podpisywanie	33					
	5.4	1.8.	Podpisywanie wsadowe	34					
	5.5.	We	eryfikacja pliku narzędziem jarsigner	35					

1. Wstęp

Niniejsza dokumentacja opisuje zagadnienia związane z certyfikatami **Certum Code Signing SimplySign**.

Przedstawione są następujące zagadnienia:

- Aktywacja certyfikatu Certum Code Signing SimplySign w Sklepie Certum;
- Uzyskanie dostępu do konta SimplySign, na które wydawany jest certyfikat Certum Code Signing SimplySign;
- Podpisywanie certyfikatem Certum Code Signing SimplySign narzędziem signtool w systemie operacyjnym Windows;
- Podpisywanie certyfikatem Certum Code Signing SimplySign narzędziem jarsigner w systemie operacyjnym Windows;

2. Wymagania formalne do wydania certyfikatu Code Signing

Wymagania odnośnie niezbędnych dokumentów i opis procesu weryfikacji przedstawione są na następującej stronie:

https://www.certum.pl/pl/wsparcie/cert_wiedza_certyfikaty_code_signing_formalnosci/

3. Aktywacja certyfikatu Code Signing SimplySign w Sklepie CERTUM

W celu aktywacji certyfikatu Code Signing SimplySign należy przejść do strony głównej Sklepu CERTUM, znajdującej się pod adresem:

https://sklep.certum.pl

		Logowanie/rejestr	racja 🕁 Koszyk	Przejdź do koszyka »
Certum	Sklep		Szukaj w sklepie	Q
Strona główna » Strona domowa				
Historia zamówień				
Dane adresowe				
Narzędzia				
Newsletter				
Wsparcie techniczne				
Wiedza				
O Certum				
Certification Authorities Websites Evenue Evenue Certification Authorities Evenue Evenu	Warunki zakupu <u>Warunki zakupu</u> <u>Reklamacje</u> <u>Regulamin</u> <u>Kontakt</u>	Szukasz najlepszych ofert Bądź na bieżąco z ofertą pro Zapisz się na newsletteri Wpisz adres e-mail	? oduktów i promocji Certum. dodaj	

Rysunek 1: Strona główna Sklepu CERTUM.

Następnie należy nacisnąć przycisk **Logowanie/rejestracja** znajdujący się w środkowo-górnej części ekranu. Wyświetlony zostanie formularz logowania do Sklepu Certum.

English Język polski Por	П					
Logowanie do systemu						
Adres e-mail	test.assecods@interia.pl					
Hasło	•••••					
	Zaloguj					
Nie pamiętasz hasła? <u>Resetuj hasło »</u> Nie pamietasz nazwy użytkownika? <u>Przypomnij nazwę użytkownika »</u>						
©All Rights Reserved to Asseco Data Systems						
Rysune	ek 2: Logowanie do Sklepu CERTUM					

Certum Powszechne Centrum Certyfikacji ul. Królowej Korony Polskiej 21, 70-486 Szczecin

Należy wprowadzić adres e-mail, który jest nazwą użytkownika i poprawne hasło. Po wprowadzeniu tych danych należy nacisnąć przycisk **Zaloguj**. Jeżeli wprowadzone dane są poprawne nastąpi zalogowanie do Sklepu CERTUM.

			test.assecods@interia.pl (Wyloguj)	₩ Koszyk	Przejdź do koszyka »
	Sklep			Szukaj w sklepie	٩
Strona główna » Moje konto » Strona do	omowa				
Kody elektroniczne					
Aktywacja certyfikatów					
Zarządzanie certyfikatami					
Historia zamówień					
Dane adresowe					
Narzędzia					
Weryfikacja domen					
Newsletter					
Wsparcie techniczne					
Wiedza					
O Certum					
Certification Automatics (WebTrust) (WebTrust)	Warunki zakupu , <u>Warunki zakupu</u> <u>Reklama</u> , <u>Regulamin Kontakt</u>	acje	Szukasz najlepszych ofert? Bądź na bieżąco z ofertą produkte Zapisz się na newsletteri	ów i promocji Certum.	
EY and EY and the EY and			Wpisz adres e-mail	dodaj	

Rysunek 3: Sklep CERTUM – konto zalogowanego Użytkownika

Następnie z bocznego Menu należy wybrać zakładkę **Aktywacja certyfikatów**. Wyświetlona zostanie lista gotowych do aktywacji, zakupionych przez Użytkownika produktów.

		test.assecods	@interia.pl (Wyloguj)	₩ Koszyk	Przejdź do koszyka
Certum	Sklep		s	zukaj w sklepie	Q
Strona główna » Moje konto » Aktyw	acja certyfikatów				
Kody elektroniczne	Aktywacja certyfikató	w			
Aktywacja certyfikatów	Nazwa usługi	Standard Code Signin	g SimplySign 🔻		
Zarządzanie certyfikatami	Status aktywacji	Certyfikat nieaktywny	•		
listoria zamówień	Numer zamówienia				
Dane adresowe	Status płatności		*		
Varzędzia	Szukaj				
Veryfikacja domen	Na podstawie art. 38 ust. 1 pkt 1 usta Klientowi przez Spółkę certyfikatu lub	wy z dnia 30 maja 2014 r. (Dz.) jego odnowienia, Klient tradi p	U. z 2004 r. o prawach konsum rawo do odstąpienia od umowy	enta informujemy, że po udos zawartej na odległość.	tępnieniu
Newsletter	Nazwa uslugi	Data zamówienia -	Numer zamówienia	Status płatności	
Wsparcie techniczne					Certyfikat
Wiedza	Standard Code Signing SimplySign, 2 lata	28 luty 2018	8c941370-17f2-4000- 99ce-99ac66ac99bb	Oczekiwanie na	nieaktywny 🥹
O Certum	Odnovienie			planose	Aktywuj
	Standard Code Signing SimplySign, 3 lata Odnowienie	28 luty 2018	52a9e92b-bcc7-4417- be48-c02e1fbc9034	Cczekiwanie na płatność 🎯	Certyfikat nieaktywny 🕑

Rysunek 4: Sklep CERTUM - Lista zakupionych przez Użytkownika produktów

Następnie, na liście należy odszukać odpowiedni produkt i nacisnąć przyciski **Aktywuj**. Wyświetlony zostanie formularz z kolejnym krokiem aktywacji wybranego produktu.

		test.assecods@interia.pl (Wylog	guj) 🕁 Koszy	k Przejdź do koszyka »
	Sklep		Szukaj w sklepie	٩
Strona główna » Moje konto » Edycja	szczegółów aktywacji			
Kody elektroniczne	Aktywacja			
Aktywacja certyfikatów	1 Zamówienia 2.Wybór met	ody 😡 3.Klucze 4.Dane 5.Potwierdzenie		
Zarządzanie certyfikatami	Nazwa usługi	Standard Code Signing Simply Sign, 2 lat	a	
Historia zamówień		Wydanie		
Dane adresowe	Wybierz sposób dostarczenia kluczy dla	lugę SimplySign 🇐		
Narzędzia	certyfikatu			
Weryfikacja domen	Dalej »			
Newsletter				
Wsparcie techniczne				
Wiedza				
O Certum				
Certification Authorities Weinfunds EVenues EVenues	Warunki zakupu <u>Warunki zakupu</u> <u>Reklamacj</u> Regulamin <u></u> Kontakt	Szukasz najlepszych ofert? Bądź na bieżąco z ofertą prod Zapisz się na newsletter! Wpisz adres e-mail	luktów i promocji Certum. dodaj	
010-2017 by Asseco Data Systems S.A.	Projekt Ideacto Wdrożenie Divante	O firmie Kont	akt Regulamin sklepu W	/arunki zakupu Mapa stro

Rysunek 5: Aktywacja certyfikatu Code Signing SimplySign

Należy nacisnąć przycisk **Dalej**. Wyświetlony zostanie formularz, w którym należy podać dane, jakie zawarte zostaną w certyfikacie.

		test.assec	ods@interia.pl (Wyloguj)	₩ Koszyk	Przejdż do koszyka »
	Sklep		Szuk	aj w sklepie	٩
Strona główna » Moje konto » Edycja	i szczegółów aktywacji				
Kody elektroniczne	Aktywacja				
Aktywacja certyfikatów	1.Zamówienia 2.Wybór mete	ody 3.Klucze 4.Dane	5.Potwierdzenie		
Zarządzanie certyfikatami	Nazwa usługi	Standard Code Sig	ning SimplySign, 2 lata		
Historia zamówień	(1000000000000000000000000000000000000	Wydanie			
Dane adresowe	Dane do certyfikatu:	9			
Narzędzia	Nazwa *		6		
Weryfikacja domen	Funkcja skrótu *	SHA-2 V	- 0		
Newsletter	Początek ważności certyfikatu	2018-03-12			
Wsparcie techniczne	Koniec ważności certyfikatu	2020-03-11			
Wiedza	Organizacja *				
D Costum	Jednostka organizacyjna				
o certain	Miejscowość	-		(Q)	
	Województwo		•		
	Email				
	« Wstecz Dalej »				
	Chief M	*Pole wymagane			

Rysunek 6: Formularz aktywacji certyfikatu Standard Code Signing SimplySign – formularz przed wypełnieniem danych

		test.assecods@interia.p	ol (Wyloguj)	₩ Koszyk	Przejdż do koszyka a
Certum	Sklep		Szuka	aj w sklepie	٩
Strona główna » Moje konto » Edycja	a szczegółów aktywacji				
Kody elektroniczne	Aktywacja				
Aktywacja certyfikatów	1.Zamówienia 2.Wybór meto	ody 3.Klucze 4.Dane 🎯 5.Potwierdzen	ie		
Zarządzanie certyfikatami	Nazwa usługi	Standard Code Signing SimplySi	gn, 2 lata		
Historia zamówień		Wydanie			
Dane adresowe	Dane do certyfikatu:				
Narzędzia	Nazwa *	Asseco Data Systems S.A.	Θ		
Weryfikacja domen	Funkcja skrótu *	SHA-2 ¥			
Newsletter	Początek ważności certyfikatu	2018-03-12			
Weparcio tochniczno	Koniec ważności certyfikatu	2020-03-11	I		
wsparcie techniczne	Organizacja *	Asseco Data Systems S.A.	0		
Wiedza	Jednostka organizacyjna	PUBIZ	9		
O Certum	Miejscowość	Szczecin	9		
	Kraj *	Polska	۲	0	
	Województwo	zachodniopomorskie 🔻 🥹			
	Email	test.assecods@interia.pl	0		
	« Wstecz Dalej »				
		*Pole wymagane			

Rysunek 7: Formularz aktywacji certyfikatu Standard Code Signing SimplySign – formularz po wypełnieniu danych

Po wypełnieniu formularza należy nacisnąć przycisk **Dalej**. Wyświetlone zostanie podsumowanie.



Rysunek 8: Podsumowanie

W podsumowaniu należy:

- Sprawdzić czy dane, które umieszczone zostaną w certyfikacie są poprawne. Jeżeli nie są to należy skorzystać z przycisku Wstecz i cofnąć się do formularz, w którym można będzie poprawić dane;
- Wybrać sposób weryfikacji:
 - Weryfikacja na podstawie dokumentów
 - Weryfikacja telefoniczna
- Zaznaczyć dwie zgody

Po wykonaniu powyższych czynności należy nacisnąć przycisk **Aktywuj**. Do CERTUM zostanie złożony Wniosek a Użytkownik otrzyma wiadomość e-mail o niezbędnych dokumentów oraz e-mail z linkiem weryfikującym.

Certum Powszechne Centrum Certyfikacji ul. Królowej Korony Polskiej 21, 70-486 Szczecin

		test.assecods	s@interia.pl (Wyloguj)	₩ Koszyk	Przejdź do koszyka
Certum	Sklep		Szi	ukaj w sklepie	Q
Strona główna » Moje konto » Aktywa	icja certyfikatów				
Kody elektroniczne	🕥 Na Twój adres został	wysłany email z linkier	n do weryfikacji		
Aktywacja certyfikatów					
Zarządzanie certyfikatami	Aktywacja certyfikatóv	w			
Historia zamówień	Nazwa usługi				
Dane adresowe	Status aktywacji		•		
Varzędzia	Numer zamówienia				
Neryfikacja domen	Status płatności		*		
Vewsletter	Szukaj				
Wsparcie techniczne	Na podstawie art. 38 ust. 1 pkt 1 ustav Klientowi przez Spółkę certyfikatu lub	wy z dnia 30 maja 2014 r. (Dz jego odnowienia, Klient traci j	.U. z 2004 r. o prawach konsumer prawo do odstapienia od umowy z	nta informujemy, że po udos awartej na odległość.	stępnieniu
Wiedza	Nazwa usługi	Data zamówienia -	Numer zamówienia	Status płatności	
O Certum					
	PDF Sign SimplySign, 3 lata Odnowienie	28 luty 2018	37052b5c-c5d2-4e90- be80-aca35d937e3d	🚨 Oczekiwanie na płatność 🎱	© Usługa aktywowana ⊌
	PDF Sign SimplySign, 3 lata		37052b5c-c5d2-4e90-	🙆 Oczekiwanie na	Ow trakcie

Rysunek 9: Informacja świadcząca o złożeniu Wniosku przez Użytkownika

Następnie użytkownik musi otworzyć swoją skrzynkę e-mail i dokonać weryfikacji adresu e-mail, poprzez kliknięcie w link weryfikujący zawarty w jednej z wiadomości z CERTUM.





Rysunek 11: Informacja o konieczności weryfikacji adresu e-mail

4. Uzyskanie dostępu do certyfikatu po jego wydaniu

Po wydaniu certyfikatu przez CERTUM, Użytkownik otrzymuje trzy wiadomości e-mail:

- wydaniu certyfikatu;
- odzyskaniu dostępu do konta SimplySign, na którym znajduje się wydany certyfikat;

Certum Powszechne Centrum Certyfikacji

• sekrecie niezbędnym do odzyskania dostępu do konta SimplySign, na którym znajduje się wydany certyfikat;



Rysunek 12: Wiadomości e-mail z CERTUM

Użytkownik na początku musi przejść do wiadomości z tzw. sekretem. Następnie musi zapisać sobie prezentowany w tej wiadomości sekret.

North Contraction of the second	ebrane	Q Szukaj		Sekret dla odzyskiwanie dostępu do usługi SimplySign	
Exercise Exerci	Centrum Certyfikacji 1.ef Cenyfikac zosal utvorozony simplysign@jikssccods.pl Corpsystement existegiu on using SimplySign Select dia odzyskiwanie dosteou do using SimplySig Select dia odzyskiwanie dosteou do using SimplySig	Pointe: Wegytike	* @ CO 1 ess.1150 doi:11.49 doi:11.49	Standburgetenested at the line of t	歯 ▼
				Gdynia. Od Lukasz Werkowski -test assecods@interia.pl Odjonieti z limeja abwo - C Do simplysign@iessecods.pl x	w Law

Rysunek 13: Wiadomość z tzw. sekretem służącym do odzyskania dostępu do konta SimplySign

Certum Powszechne Centrum Certyfikacji

Po zapisaniu/skopiowaniu sekretu, Użytkownik musi przejść do wiadomości pozwalającej odzyskać dostęp do konta SimplySign.



Rysunek 14: Wiadomość umożliwiająca odzyskanie dostępu do konta SimplySign

W wiadomości znajduje się specjalny, **jednorazowy** odnośnik pozwalający odzyskać dostęp. Po kliknięciu tego odnośnika, w przeglądarce pojawi się formularz umożliwiający odzyskanie dostępu do konta SimplySign.

	ertum		Infolinia 801 540 340 / 91 4801 340	
Odzysł	iwanie dostępu do usł	ugi SimplySign		
* P	odaj sekret podany przez operatora			
			Wyślij	
🙃 Čer	Certum Wszelkie prawa zastrzeżone V0.0.48	Listy CRL / Repozytorium / Informacje prawne	/ Polityka prywatności / Mapa serwisu	

Rysunek 15: Formularz umożliwiający odzyskanie dostępu do konta SimplySign

Certum	infolinia 801 540 340 / 91 4801 340	
Odzyskiwanie dostępu	do usługi SimplySign	
* Podaj sekret podany przez operatora		
	Wydaj	
Certum Vac.48	Listy CRL / Reporytorium / Informacje pravne / Polityka prywatności / Mapa servitau	

Rysunek 16: Formularz umożliwiający odzyskanie dostępu do konta SimplySign – wprowadzony sekret

Po wprowadzeniu poprawnego sekretu i naciśnięciu przycisku **Wyślij** wyświetlony zostanie tzw. QR Code/fotokod umożliwiający uzyskanie dostępu do konta SimplySign. Wyświetlony kod należy zeskanować w aplikacji SimplySign na urządzeniu przenośnym, zgodnie z instrukcją aplikacji SimplySign – rozdział **Reset dostępu do usługi**.

Dokumentacja dla Systemu Android dostępna jest pod następującym adresem:

https://simplysign.certum.pl/dokumentacja/android/

Dokumentacja dla Systemu iOS dostępna jest pod następującym adresem:

https://simplysign.certum.pl/dokumentacja/ios/



Rysunek 17: Odzyskiwanie dostępu do konta SimplySign – uzyskany QR Code/fotokod

5. Podpisywanie w środowisku Windows

5.1. Sprawdzenie dostępu do usługi i wyświetlenie certyfikatów

Po odzyskaniu dostępu do usługi, na urządzeniu przenośnym, w aplikacji **SimplySign** generowany jest tzw. token pozwalający na logowanie się do konta SimplySign.



Rysunek 18: Aplikacja SimplySign – wygenerowany token

W środowisku Windows, przy pomocy aplikacji **SimplySign Desktop** można sprawdzić poprawność generowania tokenów i zawartość konta SimplySign.

W celu instalacji aplikacji SimplySign Desktop dla Windows należy przejść do strony:

https://simplysign.certum.pl/pobierz/

Ze strony należy pobrać odpowiedni pakiet i zainstalować aplikację.

Po zainstalowaniu aplikacji należy ją włączyć – w tzw. tray'u – obok zegara systemowego pojawi się ikona aplikacji.



Rysunek 19: Aplikacja SimplySign Desktop – ikona

Następnie należy nacisnąć prawym klawiszy myszy na ikonę aplikacji – pojawi się menu.

Certum Powszechne Centrum Certyfikacji ul. Królowej Korony Polskiej 21, 70-486 Szczecin



Rysunek 20: Aplikacja SimplySign Desktop - menu

Należy wybrać polecenie **Połącz z SimplySign**. Pojawi się okno logowania do usługi.



Rysunek 21: Aplikacja SimplySign Desktop – logowanie do usługi

Certum Powszechne Centrum Certyfikacji ul. Królowej Korony Polskiej 21, 70-486 Szczecin

Należy wprowadzić nazwę użytkownika i token generowany na urządzeniu mobilnym i nacisnąć przycisk **Ok**. Jeżeli wprowadzone zostaną poprawne dane to nastąpi zalogowanie do usługi – wyświetlone zostanie stosowne powiadomienie z informacją o ilości kart i certyfikatów.



Rysunek 22: Aplikacja SimplySign Desktop – informacja po zalogowaniu się do usługi

Po zalogowaniu należy wyśietlić listę certyfikatów. W tym celu należy kliknąć prawym klawiszem myszy na ikonę aplikacji **SimplySign Desktop** i z menu wybrać **Zarządzanie certyfikatami** → **Lista certyfikatów**.



Rysunek 23: Aplikacja SimplySign Desktop – menu umożliwiające wyświetlenie listy certyfikatów

Nastąpi wyświetlenie listy certyfikatów.

SimplySign Desktop		Ц	
Lista certyfikatów			
Właściciel: Typ certyfikatu: Numer seryiny certyfikatu: Wystawca: Okres ważności certyfikatu: Klucz publiczny: Numer karty:	Asseco Data Systems S.A. nieznany 31 40 AF 90 25 EC 52 F1 37 32 9C F2 EB F1 03 67 Certum Class I CA SHA2 07 03 2018 - 06 03 2021 RSA, 2048 bitów 7322 7289 9537 8900 [CodeSign]		
Jiknij prawy klawisz myszy aby wy:	świetlić menu zarządzania certyfikatem		
		Zamkr	nii

Rysunek 24: Aplikacja SimplySign Desktop – lista certyfikatów

W celu wyświetlenia certyfikatu należy po prostu dwukrotnie kliknąć w jego obrębie- wyświetlone zostaną szczegóły tego certyfikatu.

🐖 Certyfikat	Х					
Ogólne Szczegóły Ścieżka certyfikacji						
Informacje o certyfikacie	-					
Ten certyfikat jest przeznaczony do:						
 Gwarantuje, że oprogramowanie pochodzi od wydawcy oprogramowania 						
Chroni oprogramowanie przed zmianą po opublikowaniu 2 23 140 1 3						
• 1.2.616.1.113527.2.5.1.7						
* Więcej informacji można znaleźć w oświadczeniu urzędu certyfikacji.						
Wystawiony dla: Asseco Data Systems S.A.						
Wystawiony przez: Certum Extended Validation Code Signing CA SHA2						
Ważny od 08.08.2017 do 07.08.2020						
Zainstaluj certyfikat Oświadczenie wystawcy						
OK						

Certum Powszechne Centrum Certyfikacji

Rysunek 25: Aplikacja SimplySign Desktop – lista certyfikatów

5.2. Podpisywanie narzędziem signtool

5.2.1. Podpis pojedynczy

W celu wykonania podpisu narzędziem signtool konieczne jest ustalenie tzw. "odcisku palca z certyfikatu". W tym celu należy wyświetlić certyfikat i przejść do zakładki Szczegóły i następnie przejść do pola Odcisk palca.

💼 Certy	fikat			×
Ogólne	Szczegóły	Ścieżka certyfik	acji	
<u>P</u> okaż:	<wszyscy></wszyscy>	•	~	
Pole			Wartość	^
Al Transformer Al	ternatywna na asady certyfika epszone użyci ternatywna na odstawowe wa życie klucza	azwa wysta atu e klucza azwa podmiotu arunki ograni	Nazwa RFC822=evcscasha2@ [1]Zasady certyfikatu:Identyfi Podpisywanie kodu (1.3.6.1.5 Inna nazwa:1.3.6.1.5.5.7.8.3 Typ podmiotu=Jednostka końc Podnis cyfrowy (80)	
	dcisk palca		f5915e3fd200f7ba5743f98ae	
f5915	e3fd200f7ba5	743f98ae8ce09	a9832fa9f7	
		Edytu	ri właściwości Kopiuj do pliku	

Rysunek 26: Szczegóły certyfikatu – wartość odcisku palca

Po uzyskaniu odcisku palca można przygotować polecenie pozwalające na podpisanie pliku. Składnia polecenia jest następująca:

signtool sign /sha1 "[1]" /tr [2] /fd [3]/v "[4]"

[1] – tzw. odcisk palca certyfikatu – w poniższym przykładzie to wartość f5915e3fd200f7ba5743f98ae8ce09a9832fa9f7

- [2] adres znacznika czasu w poniższym przykładzie to wartość http://time.certum.pl
- [3] skrót jaki zostanie użyty do podpisu w poniższym przykładzie SHA-256
- [4] ścieżka do pliku, który zostanie podpisany;

Przykładowe polecenie:

signtool sign /sha1 "f5915e3fd200f7ba5743f98ae8ce09a9832fa9f7" /tr http://time.certum.pl /fd sha256 /v "plik.exe"

W przypadku kart pinowych, po wydaniu powyższego polecenia pojawi się okno, w którym należy wprowadzić kod PIN do karty SimplySign, na której znajduje się wskazany certyfikat.



Powszechne Centrum Certyfikacji

Certum

ul. Królowej Korony Polskiej 21, 70-486 Szczecin

Rysunek 27: Aplikacja SimplySign Desktop – wprowadzanie kodu PIN do karty

W przypadku kart bezpinowych, od razu nastąpi podpisanie pliku bez podawania kodu PIN.

W obydwu przypadkach na konsoli będzie widoczny następujący stan:

```
The following certificate was selected:
    Issued to: Asseco Data Systems S.A.
    Issued by: Certum Extended Validation Code Signing CA SHA2
    Expires: Sat Mar 02 13:28:27 2019
    SHA1 hash: F5915E3FD200F7BA5743F98AE8CE09A9832FA9F7
Done Adding Additional Store
Successfully signed: plik.exe
Number of files successfully Signed: 1
Number of warnings: 0
Number of errors: 0
```

5.2.2. Podpisywanie wsadowe

W celu wsadowego podpisania wielu plików podczas jednej sesji należy w poleceniu podpisu dla atrybutu **/v** podać kolejno pliki, które mają zostać podpisane. Działanie takie eliminuje konieczność każdorazowego wywoływania komendy w konsoli oraz wpisywania kodu PIN przy podpisie kolejnych plików.

Przykładowe polecenie:

signtool sign /n "Asseco Data Systems S.A." /t http://time.certum.pl/ /fd sha1 /v aplikacja1.exe aplikacja2.exe aplikacja3.exe

W rezultacie konsola cmd.exe zwraca komunikat o poprawności podpisu plików:

```
Done Adding Additional Store
Successfully signed and timestamped: aplikacja1.exe
Successfully signed and timestamped: aplikacja2.exe
Successfully signed and timestamped: aplikacja3.exe
Number of files successfully Signed: 3
Number of warnings: 0
Number of errors: 0
```

5.2.3. Podpis dualny

Certum Powszechne Centrum Certyfikacji

W celu złożenia podpisu dualnego (wykorzystującego oba algorytmy: SHA-1 oraz SHA-2 należy przeprowadzić następującą procedurę:

1. Wykonać podpis aplikacji z wykorzystaniem algorytmu SHA-1 przykładowym poleceniem:

signtool sign /n "Asseco Data Systems S.A." /t http://time.certum.pl/ /fd sha1 /v aplikacja.exe

2. Następnie wykonać podpis tej samej aplikacji wykorzystując algorytm SHA-2 oraz przełącznik **/as**:

signtool sign /n "Asseco Data Systems S.A." /t http://time.certum.pl/ /fd sha256 /as /v aplikacja.exe

Wynikiem weryfikacji pliku podpisanego dualnie powinien być następujący komunikat z konsoli:

Do wykonania i weryfikacji podpisu dualnego wymagany jest Windows 8 lub wyższy. W celu wykonania lub weryfikacji podpisu dualnego na systemach Windows 7 należy zapoznać się z artykułem opublikowanym przez Microsoft: <u>https://technet.microsoft.com/en-us/library/security/2949927</u>.

5.3. Weryfikacja podpisu narzędziem signtool

Podpis wykonany narzędziem signtool można zweryfikować przy pomocy tego samego narzędzia. Składania takiego polecenia jest następująca:

signtool verify /pa /all [1]

[1] – nazwa weryfikowanego pliku – w przykładzie plik.exe

Przykładowe polecenie:

signtool verify /pa /all plik.exe

Po uruchomieniu przykładowego polecenia, na konsoli będzie poniższy stan:

Certum Powszechne Centrum Certyfikacji ul. Królowej Korony Polskiej 21, 70-486 Szczecin

Successfully verified: plik.exe

5.4. Podpisywanie narzędziem jarsigner

Przed rozpoczęciem używania jarsigner potrzebna jest dodatkowa konfiguracja.

5.4.4. Utworzenie pliku konfiguracyjnego provider.cfg

W pierwszym kroku należy utworzyć plik konfiguracyjny providera dla PKCS#11. W tym celu tworzymy nowy plik o rozszerzeniu *.cfg (przykład: provider.cfg). Jego zawartość wygląda następująco:

name=[1] library=[2] slotListIndex=[3]

[1] – Nazwa providera. Najlepiej SimplySignPKCS.

[2] – Ścieżka do biblioteki PKCS. Ścieżka domyślna to: C:\Windows\System32\crypto3PKCS.dll

[3] – Numer slota w którym znajduje się karta. Pierwszy slot ma numer 0, drugi numer 1 itd. W przypadku, gdy na koncie **SimplySign** jest jedna karta to należy ustawić 0. W przypadku, gdy na koncie **SimplySign** jest więcej kart, to numery slotów odpowiadają kolejno zgodnie z listą kart prezentowaną przez aplikację **SimplySign Desktop** – karta "najwyżej" ma numer slota 0. Kolejna poniżej ma numer slota 1 itd.

Uwaga!!!

Ze względu na możliwość dodawania i usuwania kart z konta SimplySign, która wpływa na kolejność slotów, przed każdym podpisem zaleca się zweryfikowanie poprawności numeru slotu.

Przykładowa konfiguracja:

name=SimplySignPKCS.dll library=C:\Windows\System32\SimplySignPKCS.dll slotListIndex=0

5.4.5. Utworzenie pliku ścieżki certyfikatu bundle.pem

Kolejnym krokiem jest utworzenie pliku ścieżki certyfikatu o rozszerzeniu*.pem (przykład: bundle.pem). Jego zawartość wygląda następująco:

- 1. "Na górze": Certyfikat użytkownika
- 2. "Poniżej": certyfikat pośredni dla certyfikatu użytkownika

UWAGA. Zawartość pliku bundle.pem musi być koniecznie we wspomnianej wyżej kolejności.

Uzyskiwanie certyfikatu Użytkownika

Aby uzyskać certyfikat użytkownika, należy po prostu go wyświetlić i przejść do zakładki Szczegóły.

Pokaż: <wszyscy></wszyscy>	~	
Pole Versja Numer servjny Algorytm podpisu Vystawca Vystawca Varity ou Podmint CN = Certum Extended Valida OU = Certum Certification Au O = Unizeto Technologies S.A C = PL	Wartość V3 63a7eed44c9a998b205b1c28 sha256RSA certum Extended Validation C piquek, z marca 2019 13:28:27 Assero Data Systems S & Pri stion Code Signing CA SHA2 thority	Warto w tym kroku zapisać sobie zawartość pola "Wystawca". Pomoże to w późniejszym doborze certyfikatu pośredniego.
	Edytuj właśdwośd	

Rysunek 28: Szczegóły certyfikatu

Następnie należy nacisnąć przycisk **Kopiuj do pliku**. Uruchomiony zostanie kreator eksportu certyfikatu.



Rysunek 29: kreator eksportu certyfikatu

Następnie należy nacisnąć przycisk **Dalej**. Wyświetlone zostanie okno umożliwiające wybranie formatu w jakim wyeksportowany zostanie certyfikat.

Format pliku eksportu Certyfikaty mogą być eksportowane w wielu różnych formatach plików. Wybierz format, którego chcesz użyć: Certyfikat X.509 szyfrowany binarnie algorytmem DER (CER) © Certyfikat X.509 szyfrowany algorytmem Base-64 (CER) O Standard składni wiadomości kryptograficznych – certyfikaty PKCS #7 (P7B) Jeśli jest to możliwe, dołącz wszystkie certyfikaty ze ścieżki certyfikacji Wymiana informacji osobistych – PKCS #12 (PFX) Jeśli jest to możliwe, dołącz wszystkie certyfikaty do ścieżki certyfikacji Usuń klucz prywatny, jeśli eksport został zakończony pomyślnie Eksportuj wszystkie właściwości rozszerzone Włącz funkcję prywatności certyfikatu	Format pliku eksportu Certyfikat y mogą być eksportowane w wielu różnych formatach plików. Wybierz format, którego chcesz użyć: Certyfikat X.509 szyfrowany binarnie algorytmem DER (CER) Ecertyfikat X.509 szyfrowany algorytmem Base-64 (CER) Standard składni wiadomości kryptograficznych – certyfikaty PKCS #7 (P7B) Jeśli jest to możliwe, dołącz wszystkie certyfikaty ze ścieżki certyfikacji Wymiana informacji osobistych – PKCS #12 (PFX) Jeśli jest to możliwe, dołącz wszystkie certyfikaty do ścieżki certyfikacji Usuń klucz prywatny, jeśli eksport został zakończony pomyślnie Eksportuj wszystkie właściwości rozszerzone Włącz funkcję prywatności certyfikatu Magazyn certyfikatów seryjnych firmy Microsoft (SST)		🖗 Kreator eksportu certyfikatów	
Wybierz format, którego chcesz użyć: Certyfikat X.509 szyfrowany binarnie algorytmem DER (CER) Ecrtyfikat X.509 szyfrowany algorytmem Base-64 (CER) Standard składni wiadomości kryptograficznych – certyfikaty PKCS #7 (P7B) Jeśli jest to możliwe, dołącz wszystkie certyfikaty ze ścieżki certyfikacji Wymiana informacji osobistych – PKCS #12 (PFX) Jeśli jest to możliwe, dołącz wszystkie certyfikaty do ścieżki certyfikacji Usuń kjucz prywatny, jeśli eksport został zakończony pomyślnie Eksportuj wszystkie właściwości rozszerzone Włącz funkcję prywatności certyfikatu	Wybierz format, którego chcesz użyć: Certyfikat X.509 szyfrowany binarnie algorytmem DER (CER) © Certyfikat X.509 szyfrowany algorytmem Base-64 (CER); O Standard składni wiadomości kryptograficznych – certyfikat PKCS #7 (P7B) Jeśli jest to możliwe, dołącz wszystkie certyfikaty ze ścieżki certyfikacji Wymiana informacji osobistych – PKCS #12 (PFX) Jeśli jest to możliwe, dołącz wszystkie certyfikaty do ścieżki certyfikacji Usuń klucz prywatny, jeśli eksport został zakończony pomyślnie Eksportuj wszystkie właściwości rozszerzone Włącz funkcję prywatności certyfikatu Magazyn certyfikatów seryjnych firmy Microsoft (SST)		Format pliku eksportu Certyfikaty mogą być eksportowane w wielu różnych formatach plików.	
 Certyfikat X.509 szyfrowany binarnie algorytmem DER (CER) Certyfikat X.509 szyfrowany algorytmem Base-64 (CER)) Standard skladni wiadomości kryptograficznych — certyfikaty PKCS #7 (P7B) Jeśli jest to możliwe, dołącz wszystkie certyfikaty ze ścieżki certyfikacji Wymiana informacji osobistych — PKCS #12 (PFX) Jeśli jest to możliwe, dgłącz wszystkie certyfikaty do ścieżki certyfikacji Usuń klucz prywatny, jeśli eksport został zakończony pomyślnie Eksportuj wszystkie właściwości rozszerzone Włącz funkcję prywatności certyfikatu 	Certyfikat X.509 szyfrowany binarnie algorytmem DER (CER) Certyfikat X.509 szyfrowany algorytmem Base-64 (CER) Standard składni wiadomości kryptograficznych — certyfikaty PKCS #7 (P7B) Jeśli jest to możliwe, dołącz wszystkie certyfikaty ze ścieżki certyfikacji Wymiana informacji osobistych — PKCS #12 (PFX) Jeśli jest to możliwe, dołącz wszystkie certyfikaty do ścieżki certyfikacji Usuń klucz prywatny, jeśli eksport został zakończony pomyślnie Eksportuj wszystkie właściwości rozszerzone Włącz funkcję prywatności certyfikatu Magazyn certyfikatów seryjnych firmy Microsoft (SST)	-	Wybierz format, którego chcesz użyć:	
Certyfikat X.509 szyfrowany algorytmem Base-64 (CER) Standard składni wiadomości kryptograficznych — certyfikaty PKCS #7 (P7B) Jeśli jest to możliwe, dołącz wszystkie certyfikaty ze ścieżki certyfikacji Wymiana informacji osobistych — PKCS #12 (PFX) Jeśli jest to możliwe, dołącz wszystkie certyfikaty do ścieżki certyfikacji Jusuń klucz prywatny, jeśli eksport został zakończony pomyślnie Eksportuj wszystkie właściwości rozszerzone Włącz funkcję prywatności certyfikatu	Ecrtyfikat X.509 szyfrowany algorytmem Base-64 (CER) Standard składni wiadomości kryptograficznych — certyfikaty PKCS #7 (P7B) Jeśli jest to możliwe, dołącz wszystkie certyfikaty ze ścieżki certyfikacji Wymiana informacji osobistych — PKCS #12 (PFX) Jeśli jest to możliwe, dołącz wszystkie certyfikaty do ścieżki certyfikacji Usuń klucz prywatny, jeśli eksport został zakończony pomyślnie Eksportuj wszystkie właściwości rozszerzone Włącz funkcję prywatności certyfikatu Magazyn certyfikatów seryjnych firmy Microsoft (SST)		Certyfikat X.509 szyfrowany binarnie algorytmem <u>D</u> ER (CER)	
 Standard składni wiadomości kryptograficznych — certyfikaty PKCS #7 (P7B) Jeśli jest to możliwe, dołącz wszystkie certyfikaty ze ścieżki certyfikacji Wymiana informacji osobistych — PKCS #12 (PFX) Jeśli jest to możliwe, dgłącz wszystkie certyfikaty do ścieżki certyfikacji Usuń Iglucz prywatny, jeśli eksport został zakończony pomyślnie Eksportuj wszystkie właściwości rozszerzone Włącz funkcję prywatności certyfikatu 	 Standard składni wiadomości kryptograficznych – certyfikaty PKCS #7 (P7B) Jeśli jest to możliwe, dołącz wszystkie certyfikaty ze ścieżki certyfikacji Wymiana informacji osobistych – PKCS #12 (PFX) Jeśli jest to możliwe, dołącz wszystkie certyfikaty do ścieżki certyfikacji Usuń klucz prywatny, jeśli eksport został zakończony pomyślnie Eksportuj wszystkie właściwości rozszerzone Włącz funkcję prywatności certyfikatu Magazyn certyfikatów seryjnych firmy Microsoft (SST) 		Certyfikat X.509 szyfrowany algorytmem Base-64 (CER)	
Jeśli jest to możliwe, dołącz wszystkie certyfikaty ze ścieżki certyfikacji <u>Wymiana informacji osobistych — PKCS #12 (PFX)</u> Jeśli jest to możliwe, d <u>o</u> łącz wszystkie certyfikaty do ścieżki certyfikacji Usuń klucz prywatny, jeśli eksport został zakończony pomyślnie Eksportuj wszystkie właściwości rozszerzone Włącz funkcję prywatności certyfikatu	 Jeśli jest to możliwe, dołącz wszystkie certyfikaty ze ścieżki certyfikacji Wymiana informacji osobistych — PKCS #12 (PFX) Jeśli jest to możliwe, dołącz wszystkie certyfikaty do ścieżki certyfikacji Usuń klucz prywatny, jeśli eksport został zakończony pomyślnie Eksportuj wszystkie właściwości rozszerzone Włącz funkcję prywatności certyfikatu Magazyn certyfikatów seryjnych firmy Microsoft (SST) 		Standard składni wiadomości kryptograficznych — certyfikaty PKCS #7 (P7B)	
 Wymiana informacji osobistych — PKCS #12 (PFX) Jeśli jest to możliwe, d<u>o</u>łącz wszystkie certyfikaty do ścieżki certyfikacji Usuń klucz prywatny, jeśli eksport został zakończony pomyślnie Eksportuj wszystkie właściwości rozszerzone Włącz funkcję prywatności certyfikatu 	 Wymiana informacji osobistych — PKCS #12 (PFX) Jeśli jest to możliwe, d<u>o</u>łącz wszystkie certyfikaty do ścieżki certyfikacji Usuń <u>k</u>lucz prywatny, jeśli eksport został zakończony pomyślnie <u>E</u>ksportuj wszystkie właściwości rozszerzone Włącz funkcję prywatności certyfikatu <u>M</u>agazyn certyfikatów seryjnych firmy Microsoft (SST) 		Jeśli jest to możliwe, dołącz wszystkie <u>c</u> ertyfikaty ze ścieżki certyfikacji	
 Jeśli jest to możliwe, d<u>o</u>łącz wszystkie certyfikaty do ścieżki certyfikacji Usuń klucz prywatny, jeśli eksport został zakończony pomyślnie Eksportuj wszystkie właściwości rozszerzone Włącz funkcję prywatności certyfikatu 	 Jeśli jest to możliwe, d<u>o</u>łącz wszystkie certyfikaty do ścieżki certyfikacji Usuń klucz prywatny, jeśli eksport został zakończony pomyślnie Eksportuj wszystkie właściwości rozszerzone Włąc<u>z</u> funkcję prywatności certyfikatu Magazyn certyfikatów seryjnych firmy Microsoft (SST) 		◯ <u>W</u> ymiana informacji osobistych — PKCS #12 (PFX)	
Usuń klucz prywatny, jeśli eksport został zakończony pomyślnie Eksportuj wszystkie właściwości rozszerzone Włącz funkcję prywatności certyfikatu	Usuń klucz prywatny, jeśli eksport został zakończony pomyślnie Eksportuj wszystkie właściwości rozszerzone Włąc <u>z</u> funkcję prywatności certyfikatu Magazyn certyfikatów seryjnych firmy Microsoft (SST)		Jeśli jest to możliwe, d <u>o</u> łącz wszystkie certyfikaty do ścieżki certyfikacji	
Eksportuj wszystkie właściwości rozszerzone Włącz funkcję prywatności certyfikatu	Eksportuj wszystkie właściwości rozszerzone Włąc <u>z</u> funkcję prywatności certyfikatu Magazyn certyfikatów seryjnych firmy Microsoft (SST)		Usuń klucz prywatny, jeśli eksport został zakończony pomyślnie	
Włącz funkcję prywatności certyfikatu	Włąc <u>z</u> funkcję prywatności certyfikatu <u>Magazyn certyfikatów seryjnych firmy Microsoft (SST) </u>		Eksportuj wszystkie właściwości rozszerzone	
	O Magazyn certyfikatów seryjnych firmy Microsoft (SST)		Włąc <u>z</u> funkcję prywatności certyfikatu	
Magazyn certyfikatów servinych firmy Microsoft (SST)			O Magazyn certyfikatów servinych firmy Microsoft (SST)	
	Dalej Anuluj		Dalej Anul	uj

Certum Powszechne Centrum Certyfikacji ul. Królowej Korony Polskiej 21, 70-486 Szczecin

Rysunek 30: kreator eksportu certyfikatu - wybór formatu certyfikatu

Należy wybrać format Base-64 i nacisnąć przycisk **Dalej**. Wyświetlone zostanie okno umożliwiające zdefiniowanie położenia wyeksportowanego pliku certyfikatu.

		×
←	F Kreator eksportu certyfikatów	
	Eksport pliku	
	Okresi nazwę piiku, ktory chcesz wyeksportowac	
	Marine -Harr	
	Nazwa piku:	
	Dalai	ui
	Datej Anu	u)

Rysunek 31: kreator eksportu certyfikatu - wskazanie ścieżki

Należy nacisnąć przycisk **Przeglądaj**. Wyświetlone zostanie okno umożliwiające nadanie nazwy eksportowanemu pliku certyfikatu.

🛃 Zapisywanie jako					¢
← → → ↑ 🔒 → Ten komputer → Dysk lokalny (C:) → c	ertyfikat		ڻ ~	Przeszukaj: certyfikat	م
Organizuj 👻 Nowy folder				1	
SSD_regi ∧ Nazwa Ten komputer Dokumenty Muzyka Obiekty 3D Obiekty 3D Obrazy Pobrane Pulpit Wideo Lysk lokalny (C:) Dysk lokalny (D:) programy (\\szc ✓	Data modyfikacji Żadne elementy nie pasuj	Typ ą do kryteriów wys	Rozmiar		
Nazwa pliku: CodeSigning					16
Zapisz jako typ: Certyfikat X.509 szyfrowany algorytmem Bas	se-64 (*.cer)				
∧ Ukryj foldery				Zapisz	Anuluj

Rysunek 32: kreator eksportu certyfikatu - wskazanie nazwy pliku

Po wskazaniu folderu docelowego i zdefiniowaniu nazwy pliku należy nacisnąć przycisk **Zapisz**. Nastąpi powrót do kreatora eksportu. Wskazana ścieżka będzie widoczna w kreatorze.

F 💱	Kreator eksportu certyfikatów	
E	i ksport pliku Określ nazwę pliku, który chcesz wyeksportować	
	<u>N</u> azwa pliku:	
	C:\certyfikat\CodeSigning.cer	Przeglądaj
		<u>D</u> alej Anul

certum.pl infolinia@certum.pl

Powszechne Centrum Certyfikacji

Certum

Rysunek 33: kreator eksportu certyfikatu - zdefiniowana lokalizacja certyfikatu

Należy nacisnąć przycisk **Dalej**. Wyświetlone zostanie ostatnie okno kreatora eksportu.

÷	<i>Ş</i> , I	Kreator eksportu certyfikatów		×
		Kończenie pracy Kreatora ekspor	tu certyfikatów	
		Praca Kreatora eksportu certyfikatów została pomy:	ślnie ukończona.	
		Wybrane zostały nastepujące ustawienia:		
		Nazwa pliku	C:\certyfikat\CodeSigning.cer	
		Eksportuj klucze	Nie	
		Dołącz wszystkie certyfikaty ze ścieżki certyfikacji	Nie	
		Format pliku	Certyfikat X.509 szyfrowany algor	
		<	>	
		5		
			Za <u>k</u> ończ Anuluj	

Rysunek 34: kreator eksportu certyfikatu - okno końcowe

Należy nacisnąć przycisk **Zakończ**. Certyfikat zostanie wyeksportowany do pliku i wyświetlony zostanie stosowny komunikat.



Rysunek 35: kreator eksportu certyfikatu - informacja o poprawnym wyeksportowaniu certyfikatu

Uzyskiwanie certyfikatu pośredniego

Certyfikaty pośrednie należy pobierać ze strony Certum:

Certum Powszechne Centrum Certyfikacji ul. Królowej Korony Polskiej 21, 70-486 Szczecin

https://www.certum.pl/pl/wsparcie/cert_wiedza_zaswiadczenia_klucze_certum/

W doborze odpowiedniego certyfikatu (certyfikatów) pośrednich pomoże zapisana wcześniej nazwa Wystawcy z pola "Wystawca" certyfikatu użytkownika. Należy odszukać na stronie Certum wystawcę swojego certyfikatu i zapisać jego certyfikat w formacie tekstowym PEM.

Następnie mając dwa pliki z certyfikatami, należy utworzyć nowy plik tekstowy. Zawartość obu uzyskanych wcześniej plików (Certyfikat użytkownika oraz certyfikat pośredni) należy wkleić do jednego pliku tekstowego we wspomnianej wyżej kolejności:

- 1. "Na górze": Certyfikat użytkownika
- 2. "Poniżej": certyfikat pośredni dla certyfikatu użytkownika

Plik należy zapisać i zmienić jego rozszerzenie na *.pem.



Rysunek 36: plik bundle

5.4.6. Uzyskanie aliasu certyfikatu

Przed przystąpieniem do podpisywania należy najpierw pozyskać tzw. alias certyfikatu. Służy do tego poniższe polecenie :

keytool	-list	-keystore	NONE	-storetype	PKCS11	–providerclass
sun.securi	ty.pkcs11	.SunPKCS11 -p	roviderArg	provider.cfg		

Certum Powszechne Centrum Certyfikacji ul. Królowej Korony Polskiej 21, 70-486 Szczecin

W rezultacie instrukcja zwraca zawartość magazynu kluczy:

Picked up _JAVA_OPTIONS: -Xms256m -Xmx1024m Enter keystore password: Keystore type: PKCS11 Keystore provider: SunPKCS11-SimplySignPKCS Your keystore contains 1 entry 63A7EED44C9A998B205B1C2850C973D7, PrivateKeyEntry, Certificate fingerprint (SHA1): F5:91:5E:3F:D2:00:F7:BA:57:43:F9:8A:E8:CE:09:A9:83:2F:A9:F7

W tym przypadku alias to:

63A7EED44C9A998B205B1C2850C973D7

5.4.7. Podpisywanie

Aby podpisać plik, w wierszu poleceń (cmd.exe) należy użyć następującego polecenia:

jarsigner -keystore NONE -tsa "[1]" -certchain "[2]" –sigalg [3] -storetype PKCS11 -providerClass sun.security.pkcs11.SunPKCS11 -providerArg "[4]" -storepass "[5]" "[6]" "[7]"

- [1] Adres znacznika czasu. Dla Certum http://time.certum.pl,
- [2] Ścieżka do pliku ścieżki certyfikatu [bundle.pem],
- [3] wskazanie algorytmu podpisu [SHA1withRSA lub SHA256withRSA],
- [4] Ścieżka do pliku konfiguracyjnego providera,

[5] – kod PIN do wirtualnej karty [dla kart <u>bezpinowych</u> należy podać <u>dowolny</u> kod PIN – nie można go pominąć w poleceniu],

- [6] Ścieżka do pliku podpisywanego,
- [7] Alias certyfikatu, którym nastąpi podpisanie pliku.

Przykładowe, poprawne polecenie:

jarsigner -keystore NONE -certchain "bundle.pem" -sigalg SHA256withRSA -tsa "http://time.certum.pl" -storetype PKCS11 -providerClass sun.security.pkcs11.SunPKCS11 -providerArg "provider.cfg" storepass "12341234" "plik.jar" "63A7EED44C9A998B205B1C2850C973D7"

Jeśli operacja podpisu przebiegła prawidłowo, konsola wyświetli następujący wynik:

Certum	ul. Królowej Korony Polskiej 21,
Powszechne Centrum Certyfikacji	70-486 Szczecin

```
Picked up _JAVA_OPTIONS: -Xms256m -Xmx1024m
jar signed.
```

5.4.8. Podpisywanie wsadowe

W celu wsadowego podpisania wielu plików podczas jednej sesji należy utworzyć plik *.bat, zawierający tyle wpisów, ile plików ma zostać podpisane podczas jednego procesu podpisu. Działanie takie eliminuje konieczność każdorazowego wywoływania komendy w konsoli oraz wpisywania kodu PIN przy podpisie kolejnych plików.

W celu utworzenia pliku, należy utworzyć nowy plik tekstowy *.txt, wkleić wpisy do podpisywania plików, zapisać plik oraz zmienić jego rozszerzenie z *.txt na *.bat.

Poniższy przykład prezentuje zawartość pliku *.bat dla podpisu trzech aplikacji jednocześnie:

```
jarsigner -keystore NONE -certchain "bundle.pem" -tsa "http://time.certum.pl" -
storetype PKCS11 -providerClass sun.security.pkcs11.SunPKCS11 -providerArg
"provider.cfg" -storepass "12341234" "aplikacja1.jar"
"63A7EED44C9A998B205B1C2850C973D7
jarsigner -keystore NONE -certchain "bundle.pem" -tsa "http://time.certum.pl" -
storetype PKCS11 -providerClass sun.security.pkcs11.SunPKCS11 -providerArg
"provider.cfg" -storepass "12341234" "aplikacja2.jar"
"63A7EED44C9A998B205B1C2850C973D7
jarsigner -keystore NONE -certchain "bundle.pem" -tsa "http://time.certum.pl" -
storetype PKCS11 -providerClass sun.security.pkcs11.SunPKCS11 -providerArg
"provider.cfg" -storepass "12341234" "aplikacja2.jar"
"63A7EED44C9A998B205B1C2850C973D7
jarsigner -keystore NONE -certchain "bundle.pem" -tsa "http://time.certum.pl" -
storetype PKCS11 -providerClass sun.security.pkcs11.SunPKCS11 -providerArg
"provider.cfg" -storepass "12341234" "aplikacja3.jar"
"63A7EED44C9A998B205B1C2850C973D7"
```

Tak zapisany plik można uruchomić w konsoli cmd.exe lub dwuklikiem, a rezultatem będzie rozpoczęcie podpisywania kolejnych plików, zawartych w pliku *.bat.

Rezultatem uruchomienia pliku *.bat w konsoli będzie informacja o kolejnym wywołaniu komend i podpisie plików:

C:\Users\user\Desktop\jarsigner>jarsigner -keystore NONE -certchain "bundle.pem" -tsa http://time.certum.pl -storetype PKCS11 providerClass sun.security.pkcs11.SunPKCS11 -providerArg "provider.cfg" -storepass "12341234" "aplikacja1.jar" "63A7EED44C9A998B205B1C2850C973D7"

Certum	ul. Królowej Korony Polskiej 21,	certum.p
Powszechne Centrum Certyfikacji	70-486 Szczecin	infolinia@certum.p

Picked up _JAVA_OPTIONS: -Xms256m -Xmx1024m
jar signed.

```
C:\Users\user\Desktop\jarsigner>jarsigner -keystore NONE -certchain
"bundle.pem" -tsa http://time.certum.pl -storetype PKCS11
providerClass
               sun.security.pkcs11.SunPKCS11
                                                -providerArg
"provider.cfg" -storepass
                                 "12341234" "aplikacja2.jar"
"63A7EED44C9A998B205B1C2850C973D7"
Picked up JAVA OPTIONS: -Xms256m -Xmx1024m
jar signed.
C:\Users\user\Desktop\jarsigner>jarsigner -keystore NONE -certchain
"bundle.pem" -tsa http://time.certum.pl -storetype PKCS11
providerClass
                 sun.security.pkcs11.SunPKCS11
                                                    -providerArg
"provider.cfg" -storepass
                                 "12341234"
                                                 "aplikacja3.jar"
"63A7EED44C9A998B205B1C2850C973D7"
```

Picked up _JAVA_OPTIONS: -Xms256m -Xmx1024m jar signed.

5.5. Weryfikacja pliku narzędziem jarsigner

Weryfikacja podpisanego pliku, przy użyciu narzędzia jarsignier odbywa się następującym poleceniem:

jarsigner -verify "[1]"

[1] – Ścieżka do pliku podpisywanego,

Przykładowe, poprawne polecenie:

jarsigner -verify "plik.jar"

W przypadku poprawnej weryfikacji pliku konsola wyświetli:

Picked up JAVA OPTIONS: -Xms256m -Xmx1024m

jar verified.

W przypadku braku podpisu wynik jest następujący:

Picked up JAVA OPTIONS: -Xms256m -Xmx1024m

jar is unsigned.

Certum Powszechne Centrum Certyfikacji ul. Królowej Korony Polskiej 21, 70-486 Szczecin