

Certum Code Signing

Instrukcja certyfikatu Code Signing SimplySign

Wersja 1.0

Spis treści

1. Wstęp.....	3
2. Wymagania formalne do wydania certyfikatu Code Signing.....	3
3. Aktywacja certyfikatu Code Signing SimplySign w Sklepie CERTUM	3
4. Uzyskanie dostępu do certyfikatu po jego wydaniu.....	12
5. Podpisywanie w środowisku Windows	16
5.1. Sprawdzenie dostępu do usługi i wyświetlenie certyfikatów	16
5.2. Podpisywanie narzędziem signtool.....	21
5.2.1. Podpis pojedynczy	21
5.2.2. Podpisywanie wsadowe.....	23
5.2.3. Podpis dualny	23
5.3. Weryfikacja podpisu narzędziem signtool.....	24
5.4. Podpisywanie narzędziem jarsigner	25
5.4.4. Utworzenie pliku konfiguracyjnego provider.cfg.....	25
5.4.5. Utworzenie pliku ścieżki certyfikatu bundle.pem	26
5.4.6. Uzyskanie aliasu certyfikatu	32
5.4.7. Podpisywanie	33
5.4.8. Podpisywanie wsadowe.....	34
5.5. Weryfikacja 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

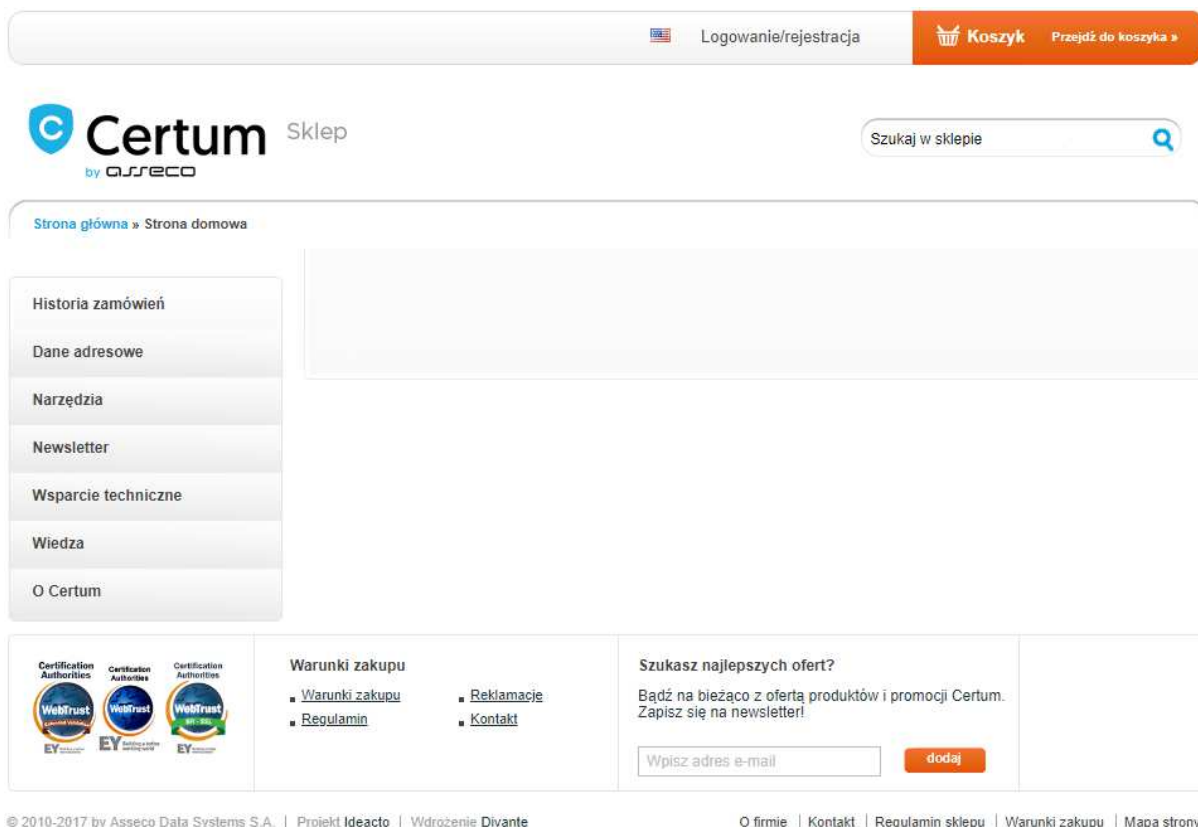
Wymagania odnośnie niezbędnych dokumentów i opis procesu weryfikacji przedstawione są na następującej stronie:

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>



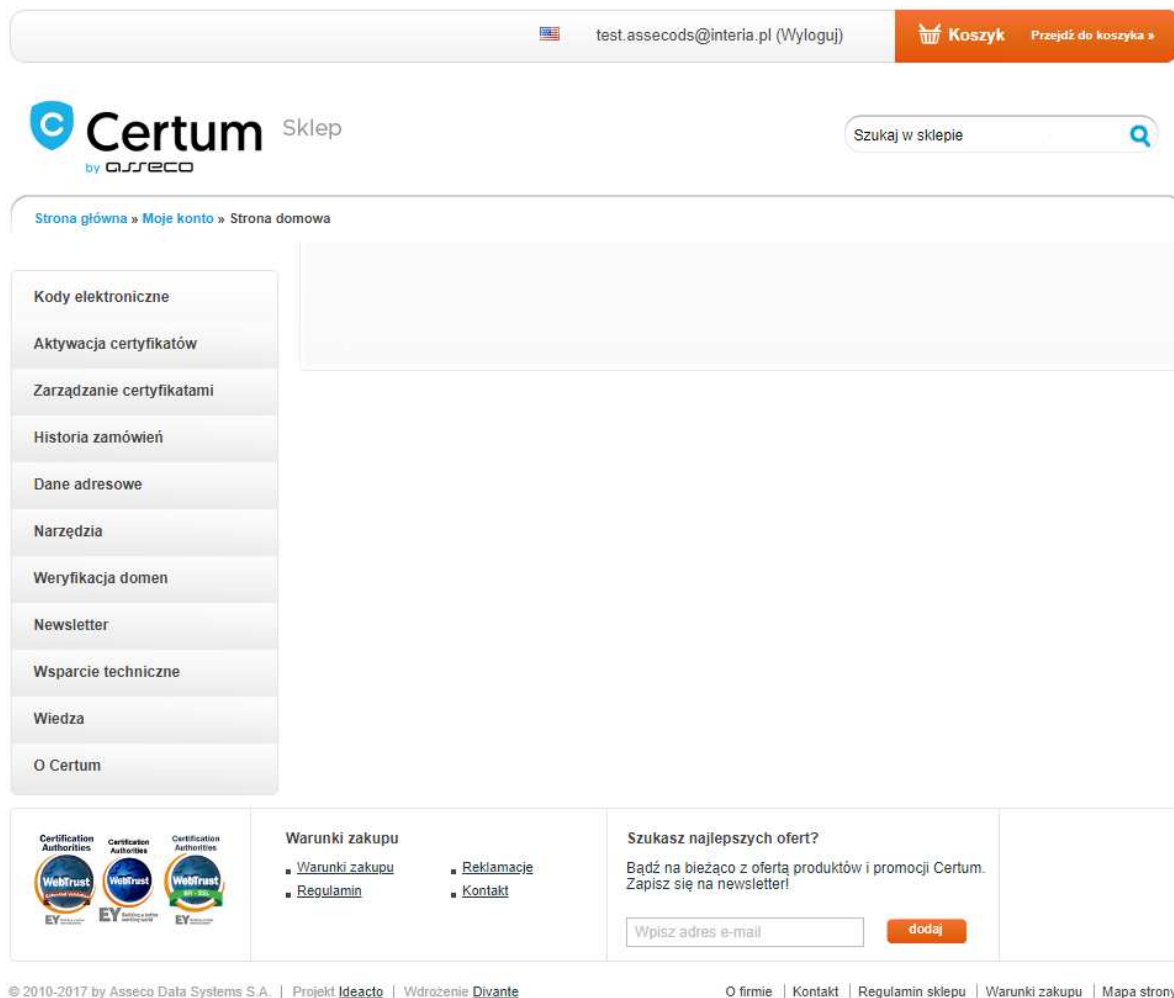
Rysunek 1: Strona główna Sklepu CERTUM.

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

The screenshot shows the Certum login page. At the top, there's the Certum logo with 'by asseco' and language selection links: 'English', 'Język polski', and 'Россию'. Below this is the heading 'Logowanie do systemu'. The login form consists of two input fields: 'Adres e-mail' with the value 'test.assecods@interia.pl' and 'Hasło' with a masked password '.....'. A red 'Zaloguj' button is positioned below the fields. Below the button, there are two links: 'Nie pamiętasz hasła? [Resetuj hasło »](#)' and 'Nie pamiętasz nazwy użytkownika? [Przypomnij nazwę użytkownika »](#)'. The footer contains the copyright information '©All Rights Reserved to Asseco Data Systems'.

Rysunek 2: Logowanie do Sklepu CERTUM

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.



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.


Certum Sklep
by asseco

[test.assecods@interia.pl \(Wyloguj\)](#)


Koszyk

[Przejdź do koszyka »](#)

[Strona główna »](#)
[Moje konto »](#)
[Aktywacja certyfikatów](#)

Kody elektroniczne

Aktywacja certyfikatów

Zarządzanie certyfikatami

Historia zamówień

Dane adresowe

Narzędzia

Weryfikacja domen

Newsletter

Wsparcie techniczne

Wiedza

O Certum

Aktywacja certyfikatów

Nazwa usługi: Standard Code Signing SimplySign ▼

Status aktywacji: Certyfikat nieaktywny ▼

Numer zamówienia:

Status płatności: ▼

Szukaj

Na podstawie art. 38 ust. 1 pkt 1 ustawy z dnia 30 maja 2014 r. (Dz.U. z 2004 r. o prawach konsumenta informujemy, że po udostępnieniu Klientowi przez Spółkę certyfikatu lub jego odnowienia, Klient traci prawo do odstąpienia od umowy zawartej na odległość.

Nazwa usługi	Data zamówienia ▼	Numer zamówienia	Status płatności	
Standard Code Signing Simply Sign, 2 lata Odnowienie	28 luty 2018	8c941370-17f2-4000-99ce-99ac66ac99bb	 Oczekiwanie na płatność ⓘ	Certyfikat nieaktywny ⓘ Aktywuj
Standard Code Signing Simply Sign, 3 lata Odnowienie	28 luty 2018	52a9e92b-bcc7-4417-be48-c02e1fbc9034	 Oczekiwanie na płatność ⓘ	Certyfikat nieaktywny ⓘ Aktywuj

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.


Certum Sklep
by asseco

[test.aseccods@interia.pl \(Wyloguj\)](#)
[Koszyk](#) [Przejdź do koszyka >](#)

[Szukaj w sklepie](#)

[Strona główna >](#)
[Moje konto >](#)
Edycja szczegółów aktywacji

Kody elektroniczne
Aktywacja certyfikatów
Zarządzanie certyfikatami
Historia zamówień
Dane adresowe
Narzędzia
Weryfikacja domen
Newsletter
Wsparcie techniczne
Wiedza
O Certum

Aktywacja

1. Zamówienia 2. Wybór metody 3. Klucze 4. Dane 5. Potwierdzenie

Nazwa usługi **Standard Code Signing SimplySign, 2 lata**
Wydanie

Wybierz sposób dostarczenia kluczy dla certyfikatu

☒ generowanie kluczy na karcie przez usługę SimplySign

[Dalej >>](#)





Warunki zakupu

- [Warunki zakupu](#)
- [Regulamin](#)

- [Reklamacje](#)
- [Kontakt](#)

Szukasz najlepszych ofert?
 Bądź na bieżąco z ofertą produktów i promocji Certum. Zapisz się na newsletter!

[dodaj](#)

© 2010-2017 by Asseco Data Systems S.A. | Projekt [Ideacto](#) | Wdrożenie [Divante](#)

[O firmie](#) | [Kontakt](#) | [Regulamin sklepu](#) | [Warunki zakupu](#) | [Mapa strony](#)

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.assecods@interia.pl (Wyloguj)

KoszykPrzejdź do koszyka »

 **Certum** Sklep
by asseco

Szukaj w sklepie

Strona główna » Moje konto » Edycja szczegółów aktywacji

Kody elektroniczne

Aktywacja certyfikatów

Zarządzanie certyfikatami

Historia zamówień

Dane adresowe

Narzędzia

Weryfikacja domen

Newsletter

Wsparcie techniczne

Wiedza

O Certum

Aktywacja

1. Zamówienia 2. Wybór metody 3. Klucze 4. Dane 5. Potwierdzenie

Nazwa usługi **Standard Code Signing SimplySign, 2 lata**
Wydanie

Dane do certyfikatu:

Nazwa *

Funkcja skrótu *SHA-2

Początek ważności certyfikatu2018-03-12

Koniec ważności certyfikatu2020-03-11

Organizacja *

Jednostka organizacyjna

Miejscowość

Kraj *

Województwo

Email

« Wstecz

Dalej »

*Pole wymagane

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

test.assecods@interia.pl (Wyloguj)

Koszyk [Przejdź do koszyka »](#)

Certum Sklep
by asseco

Szukaj w sklepie

[Strona główna](#) » [Moje konto](#) » Edycja szczegółów aktywacji

Kody elektroniczne

Aktywacja certyfikatów

Zarządzanie certyfikatami

Historia zamówień

Dane adresowe

Narzędzia

Weryfikacja domen

Newsletter

Wsparcie techniczne

Wiedza

O Certum

Aktywacja

1. Zamówienia 2. Wybór metody 3. Klucze 4. Dane 5. Potwierdzenie

Nazwa usługi **Standard Code Signing SimplySign, 2 lata**
Wydanie

Dane do certyfikatu:

Nazwa *

Asseco Data Systems S.A.

Funkcja skrótu *

SHA-2

Początek ważności certyfikatu

2018-03-12

Koniec ważności certyfikatu

2020-03-11

Organizacja *

Asseco Data Systems S.A.

Jednostka organizacyjna

PUBIZ

Miejscowość

Szczecin

Kraj *

Polska

Województwo

zachodniopomorskie

Email

test.assecods@interia.pl

« 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.

© 2016-2017 by Asseco Data Systems S.A. | Projekt Ideacto | Wdrożenie Divante

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.


[test.assecods@interia.pl \(Wyloguj\)](#)


[Koszyk](#)
[Przejdź do koszyka »](#)


Certum Sklep
by asseco



[Strona główna »](#)
[Moje konto »](#)
Aktywacja certyfikatów

Kody elektroniczne
Aktywacja certyfikatów
Zarządzanie certyfikatami
Historia zamówień
Dane adresowe
Narzędzia
Weryfikacja domen
Newsletter
Wsparcie techniczne
Wiedza
O Certum


Na Twój adres został wysłany email z linkiem do weryfikacji

Aktywacja certyfikatów

Nazwa usługi

Status aktywacji

Numer zamówienia

Status płatności

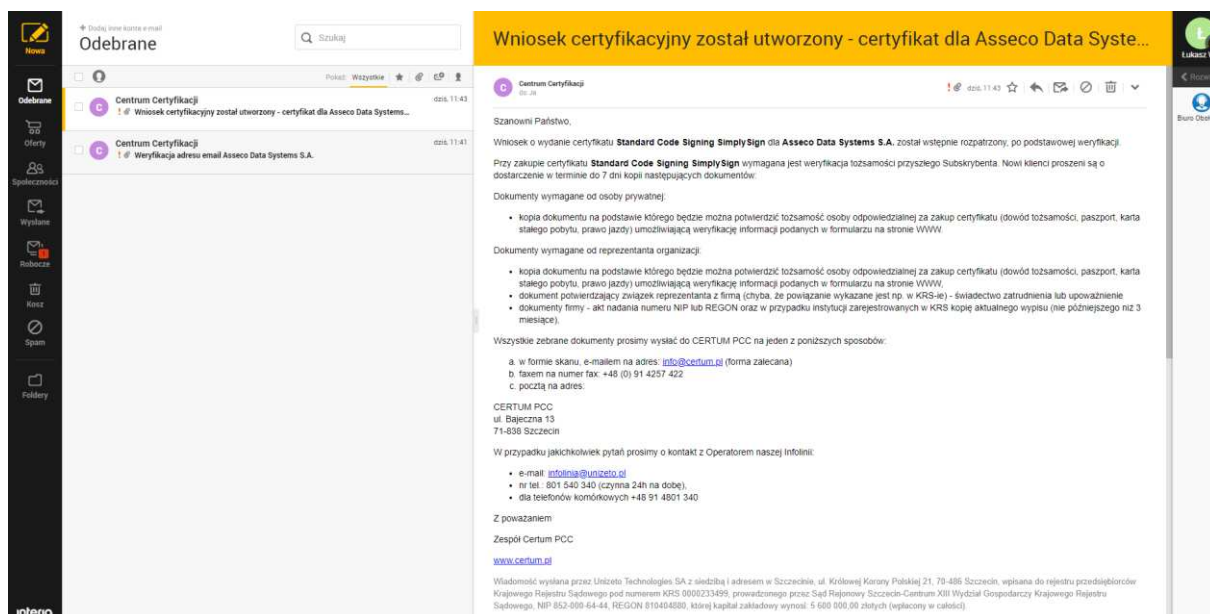
Szukaj

Na podstawie art. 38 ust. 1 pkt 1 ustawy z dnia 30 maja 2014 r. (Dz.U. z 2004 r. o prawach konsumenta informujemy, że po udostępnieniu Klientowi przez Spółkę certyfikatu lub jego odnowienia, Klient traci prawo do odstąpienia od umowy zawartej na odległość.

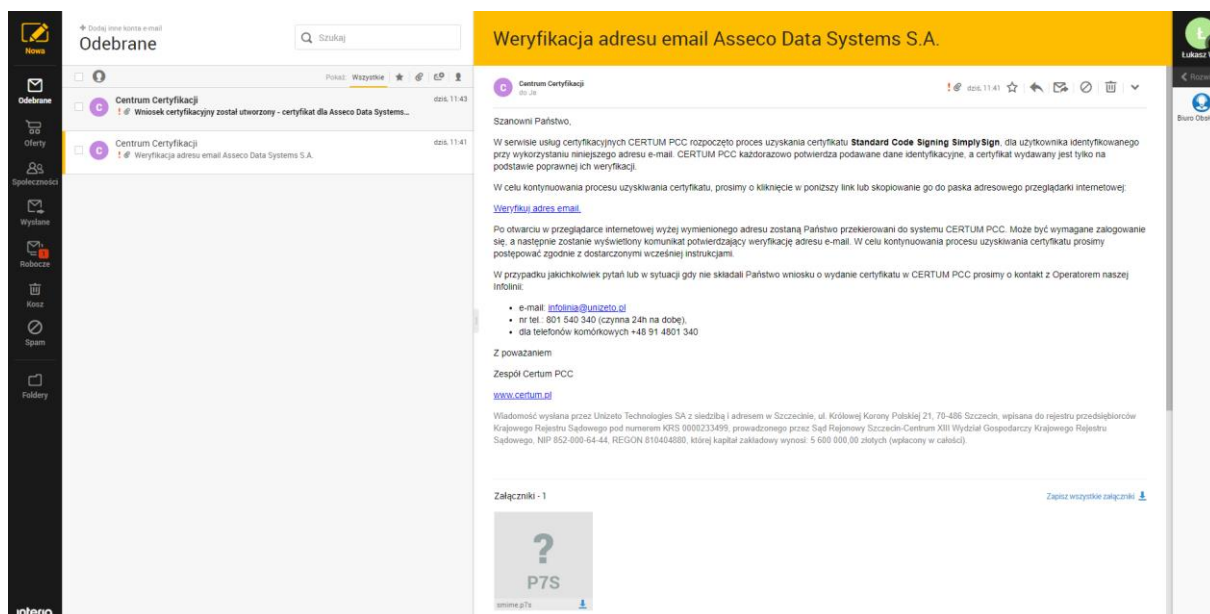
Nazwa usługi	Data zamówienia	Numer zamówienia	Status płatności	
PDF Sign SimplySign, 3 lata Odnowienie	28 luty 2018	37052b5c-c5d2-4e90-be80-aca35d937e3d	Oczekiwanie na płatność	 Usługa aktywowana
PDF Sign SimplySign, 3 lata Wydanie	28 luty 2018	37052b5c-c5d2-4e90-be80-aca35d937e3d	Oczekiwanie na płatność	 W trakcie realizacji

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 10: Informacja o złożeniu Wniosku



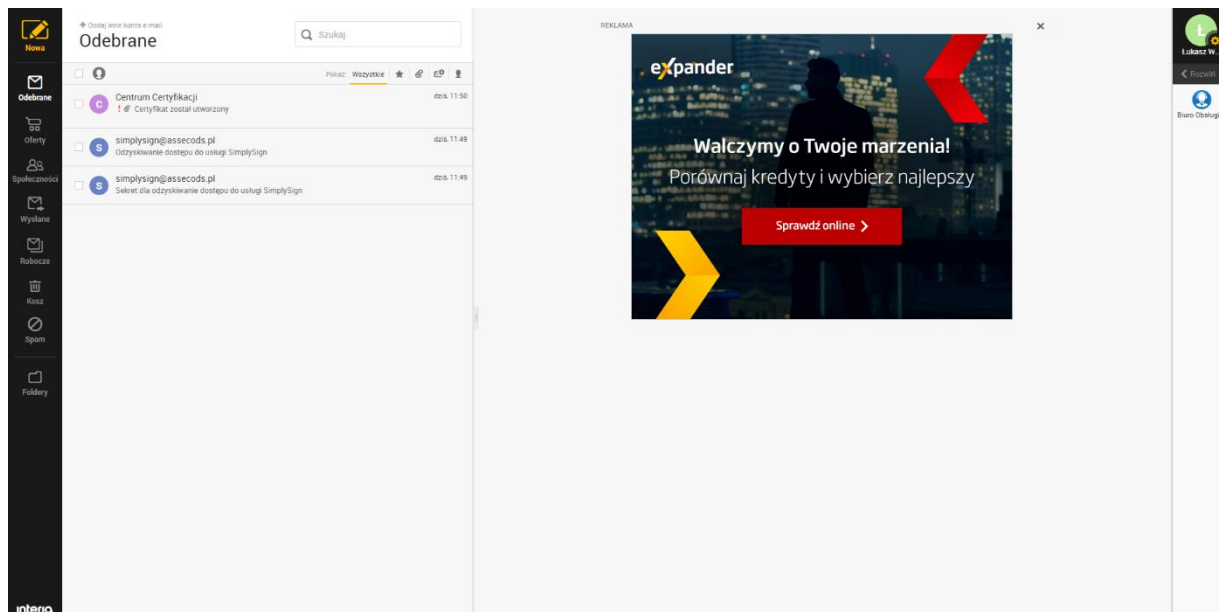
Rysunek 11: Informacja o konieczności weryfikacji adresu e-mail

4. Uzyskanie dostępu do certyfikatu po jego wydaniu

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

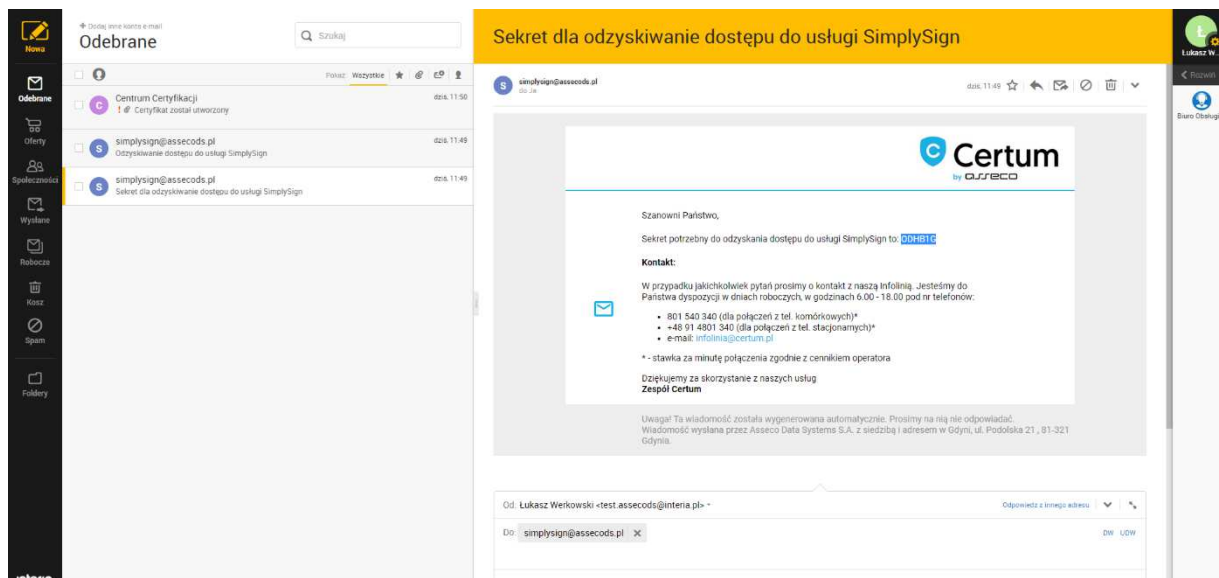
- wydaniu certyfikatu;
- odzyskaniu dostępu do konta SimplySign, na którym znajduje się wydany certyfikat;

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



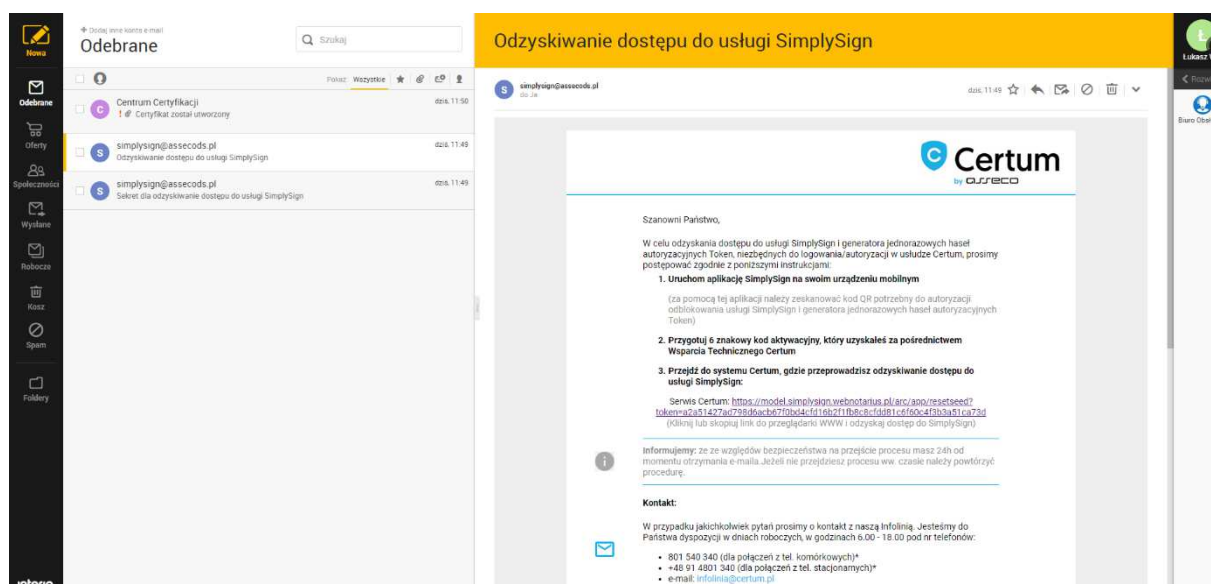
Rysunek 12: Wiadomości e-mail z CERTUM

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



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

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.

Rysunek 15: Formularz umożliwiający odzyskanie dostępu do konta SimplySign

Certum
by ORSECO

Infolinia 801 540 340 / 91 4801 340

Odzyskiwanie dostępu do usługi SimpleSign

* Podaj sekret podany przez operatora

Wyślij

ORSECO
DATA SYSTEMS

Powszechne Centrum Certyfikacji

Certum
Wszystkie prawa zastrzeżone
v0.0.48

[Listy CRL](#) / [Repozytorium](#) / [Informacje prawne](#) / [Polityka prywatności](#) / [Mapa serwisu](#)

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

Po wprowadzeniu poprawnego sekretu i naciśnięciu przycisku **Wyślij** wyświetlony zostanie tzw. QR Code/fotokod umożliwiający uzyskanie dostępu do konta SimpleSign. Wyświetlony kod należy zeskanować w aplikacji SimpleSign na urządzeniu przenośnym, zgodnie z instrukcją aplikacji SimpleSign – 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 SimpleSign – 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 **SimpleSign** generowany jest tzw. token pozwalający na logowanie się do konta SimpleSign.



Rysunek 18: Aplikacja SimplySign – wygenerowany token

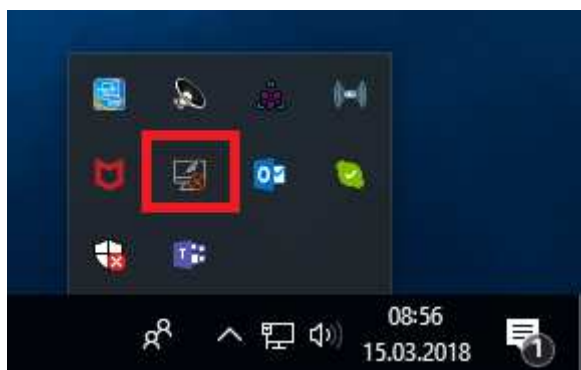
W środowisku Windows, przy pomocy aplikacji **SimplySign Desktop** można sprawdzić poprawność generowania tokenów i zawartość konta SimplySign.

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

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

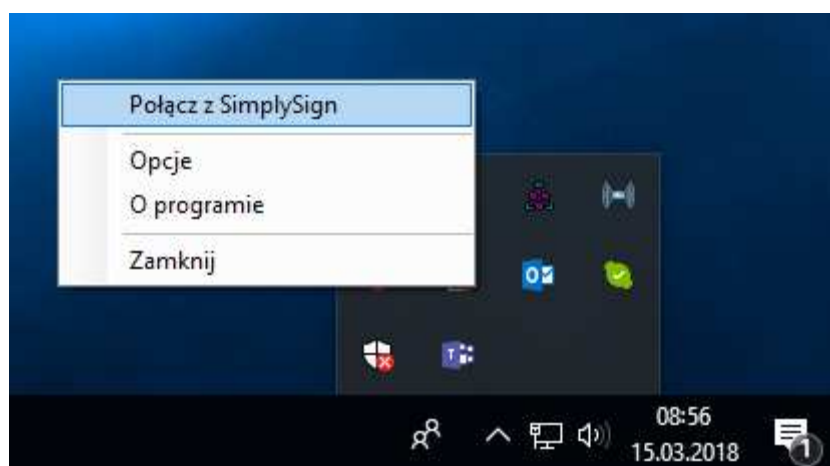
Ze strony należy pobrać odpowiedni pakiet i zainstalować aplikację.

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 klawiszem myszy na ikonę aplikacji – pojawi się menu.

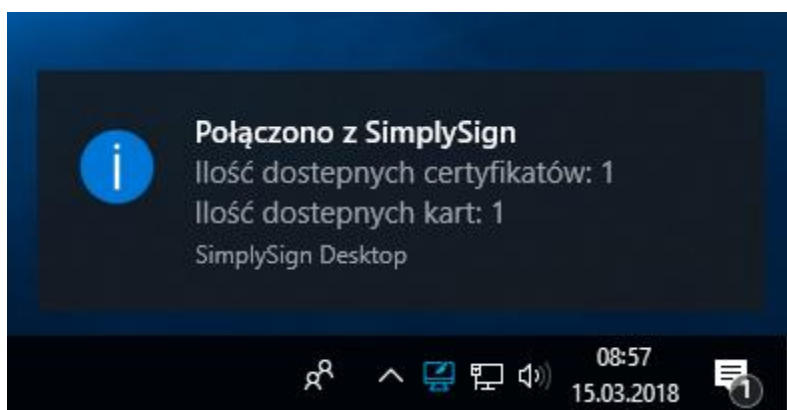


Rysunek 20: Aplikacja SimplySign Desktop – menu

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

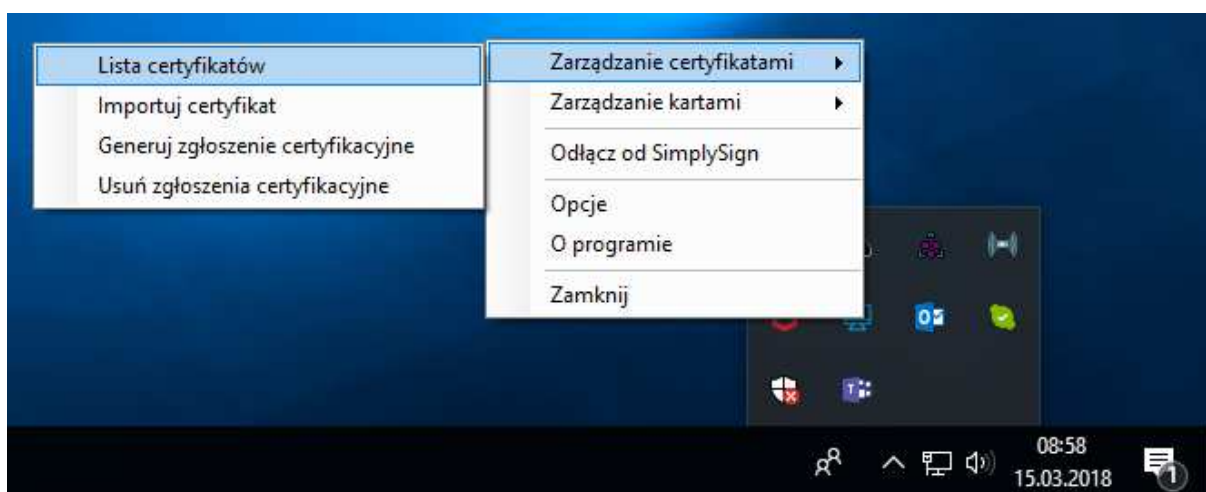
Rysunek 21: Aplikacja SimplySign Desktop – logowanie do usługi

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.



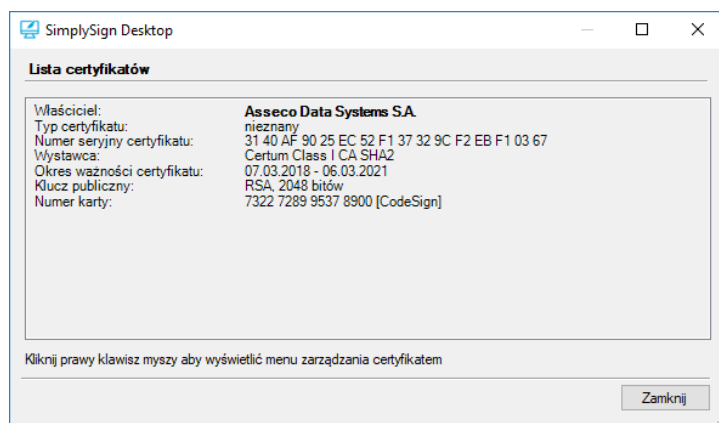
Rysunek 22: Aplikacja SimplySign Desktop – informacja po zalogowaniu się do usługi

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



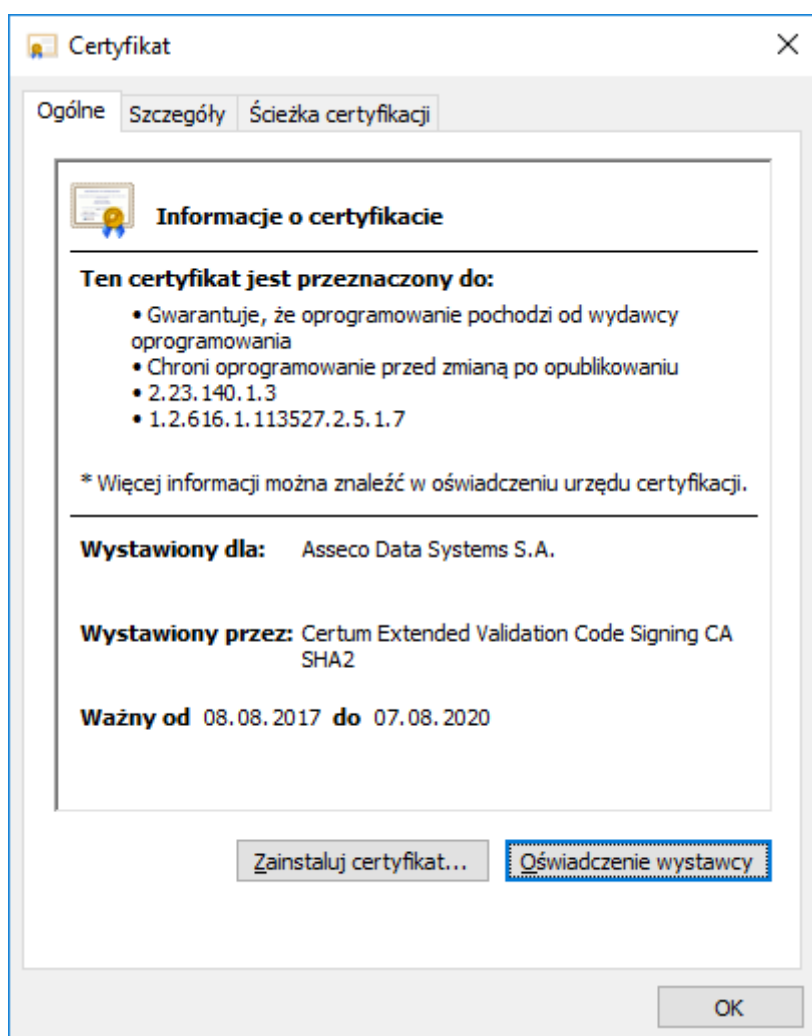
Rysunek 23: Aplikacja SimplySign Desktop – menu umożliwiające wyświetlenie listy certyfikatów

Nastąpi wyświetlenie listy certyfikatów.



Rysunek 24: Aplikacja SimplySign Desktop – lista certyfikatów

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

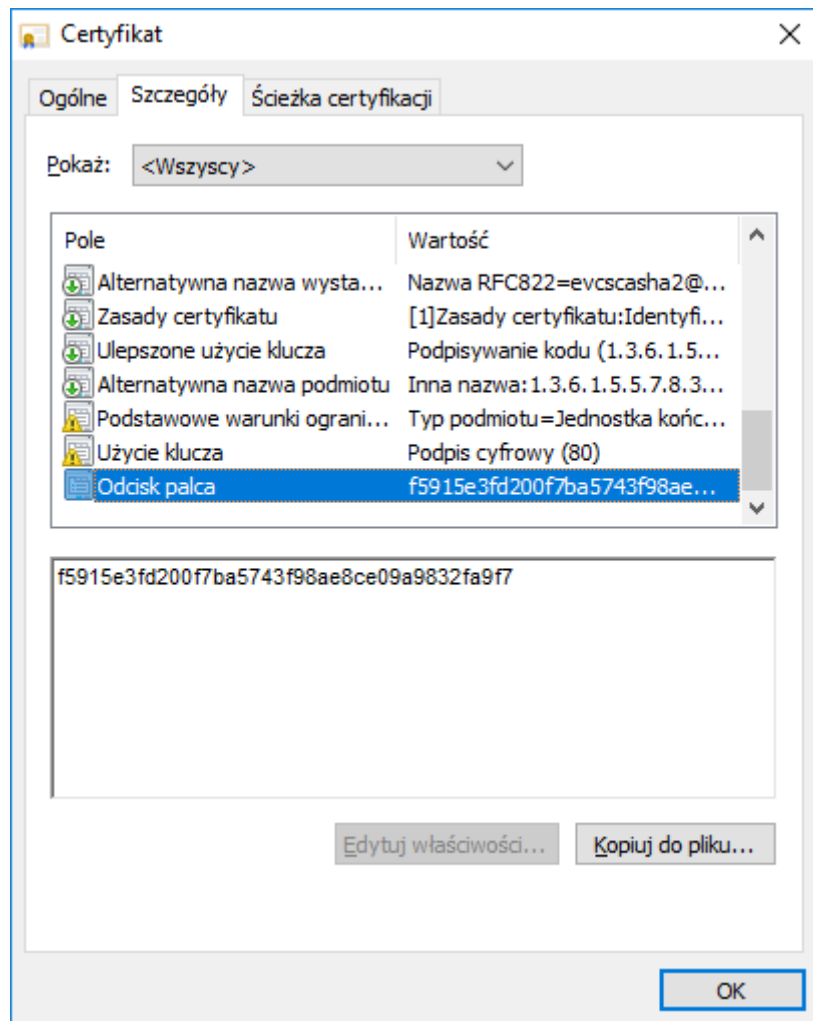


Rysunek 25: Aplikacja SimplySign Desktop – lista certyfikatów

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**.



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.

The screenshot shows a Windows-style dialog box titled "Logowanie do karty" (Card Login). Inside, the "SimplySign Desktop by ASSECO" logo is prominent. Below it, a section titled "Dane karty" (Card Data) lists the following information:

Nazwa użytkownika:	certum.cloudfest2018@gmail.com
Numer karty:	7371 7090 8757 6629
Nazwa karty:	SimplySignPIN

Below the card data, there is a label "Podaj PIN:" followed by a text input field. Underneath the input field, it says "Ilość dostępnych prób: 3". At the bottom of the window, there are two buttons: "Ok" and "Anuluj". The version number "KSP v. 1.2.0.9" is displayed in the bottom right corner.

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

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:

```
File: aplikacja.exe
Index  Algorithm  Timestamp
=====
0      sha1      Authenticode
1      sha256    RFC3161

Successfully verified: aplikacja.exe
```

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: <https://technet.microsoft.com/en-us/library/security/2949927>.

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:


```
File: plik.exe
Index  Algorithm  Timestamp
=====
0      sha256     RFC3161
```

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 slotu 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 slotu 0. Kolejna poniżej ma numer slotu 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

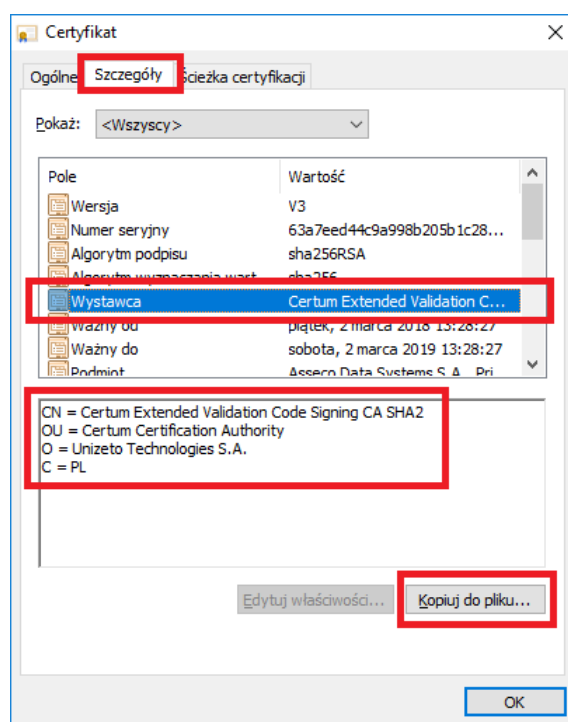
Kolejnym krokiem jest utworzenie pliku ścieżki certyfikatu o rozszerzeniu*.pem (przykład: bundle.pem). Jego zawartość wygląda następująco:

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

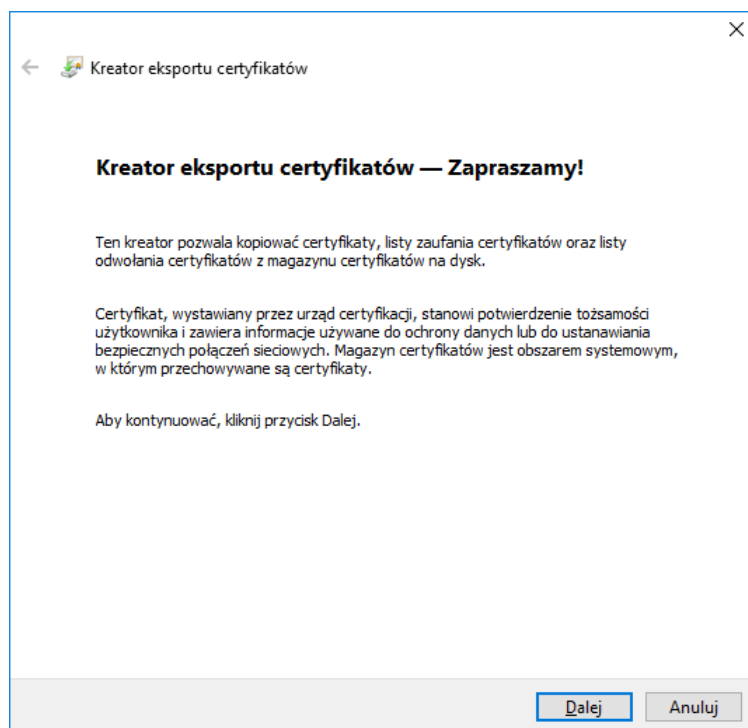
Aby uzyskać certyfikat użytkownika, należy po prostu go wyświetlić i przejść do zakładki **Szczegóły**.



Warto w tym kroku zapisać sobie zawartość pola „Wystawca”. Pomoże to w późniejszym doborze certyfikatu pośredniego.

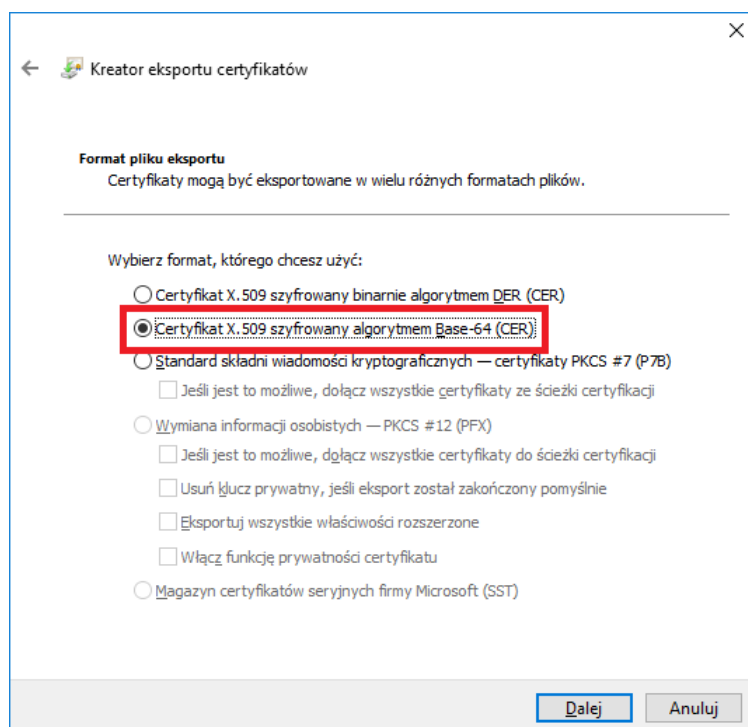
Rysunek 28: Szczegóły certyfikatu

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



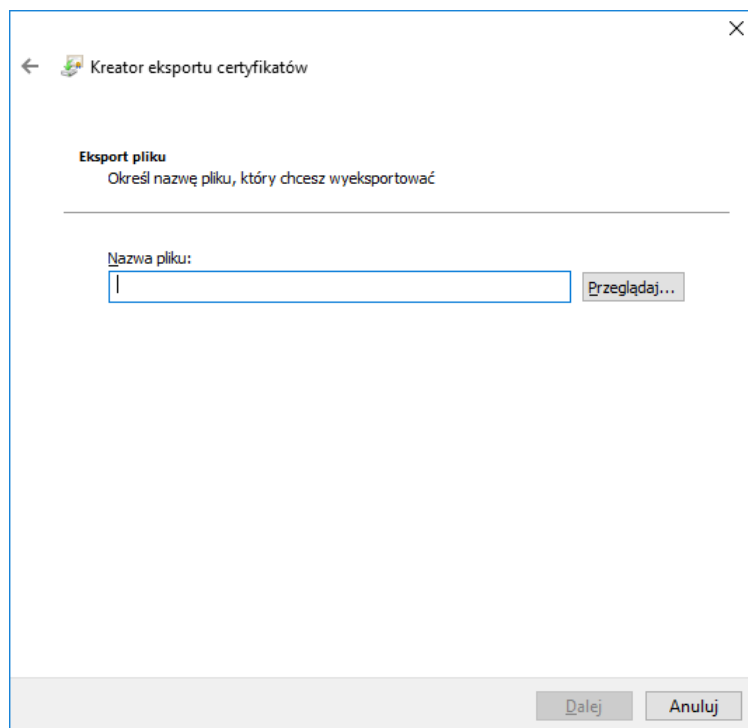
Rysunek 29: kreator eksportu certyfikatu

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



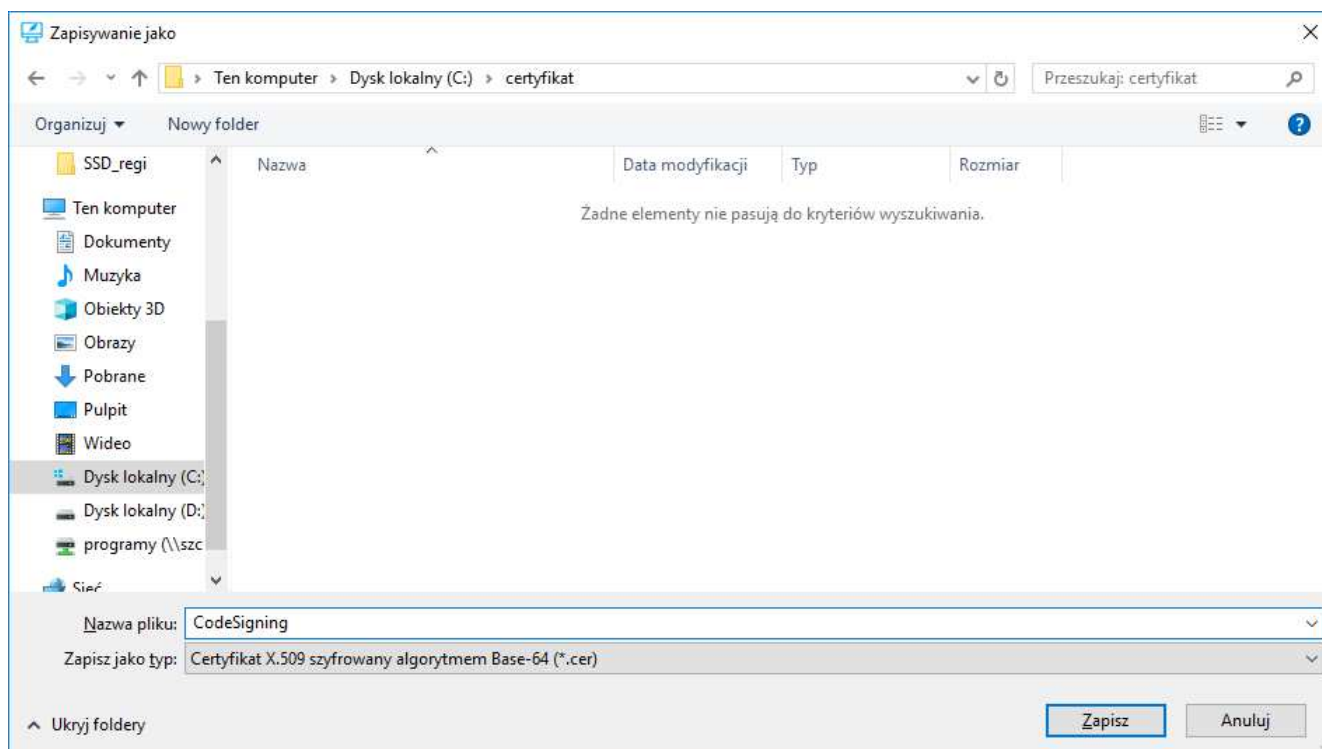
Rysunek 30: kreator eksportu certyfikatu – wybór formatu certyfikatu

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



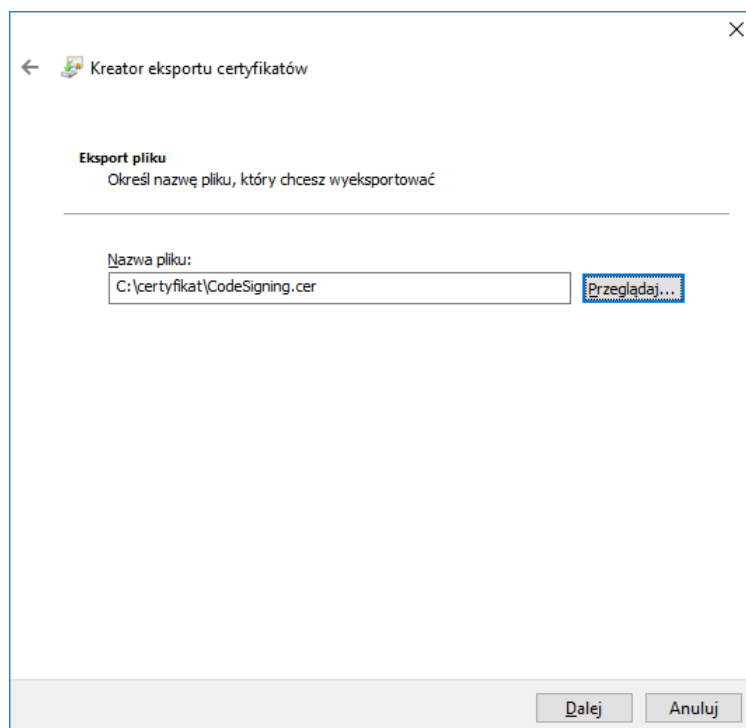
Rysunek 31: kreator eksportu certyfikatu – wskazanie ścieżki

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



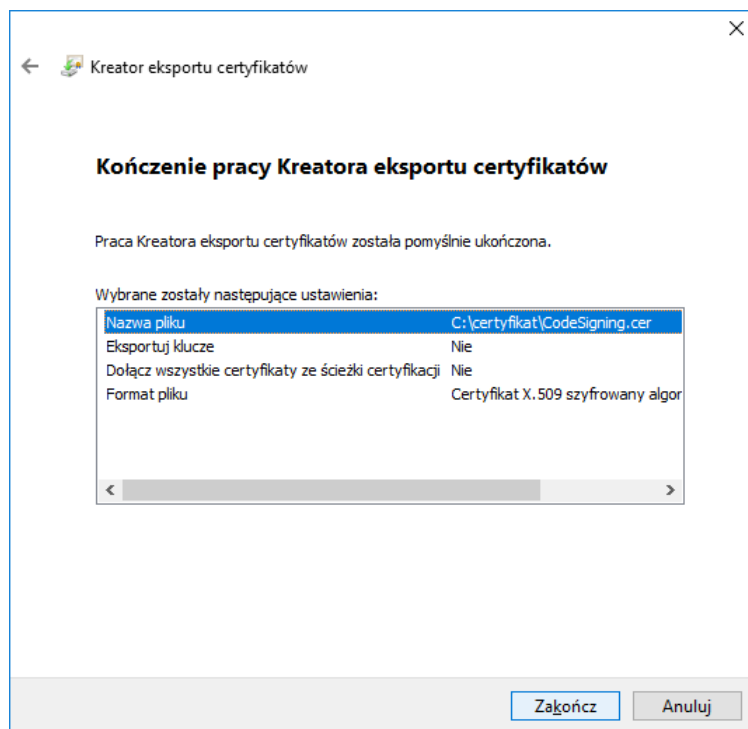
Rysunek 32: kreator eksportu certyfikatu – wskazanie nazwy pliku

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



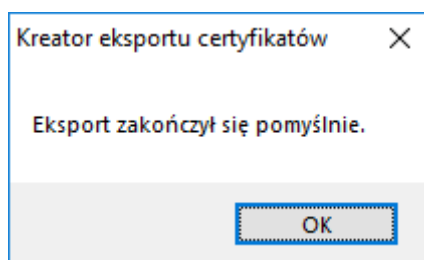
Rysunek 33: kreator eksportu certyfikatu – zdefiniowana lokalizacja certyfikatu

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



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

certum.pl
infolinia@certum.pl

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.

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 bezipinowych należy podać dowolny 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:

```
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" "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"
```

```
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 jarsigner 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.
```