Podpisywanie kodu przy użyciu narzędzi Signtool oraz Jarsigner

Certum Code Signing

Spis treści

1 Opis produktu

Certyfikat **Code Signing**, służy do podpisywania kodu oraz gotowych już zbudowanych aplikacji. Certyfikat nagrywany jest na **kartę kryptograficzną**, co pozwala nam podpisywać kod oraz gotowe aplikacje używając znanych narzędzi takich jak ***Signtool.exe*** oraz ***Jarsigner***.

Instrukcja opisuje użycie narzędzi Signtool oraz Jarsigner w celu podpisania kodu.

2 Signtool

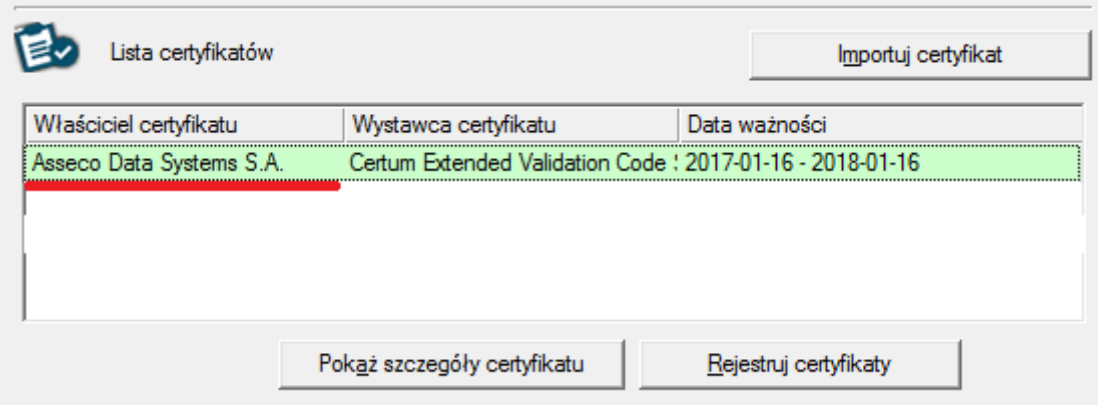
2.1 Opis narzędzia

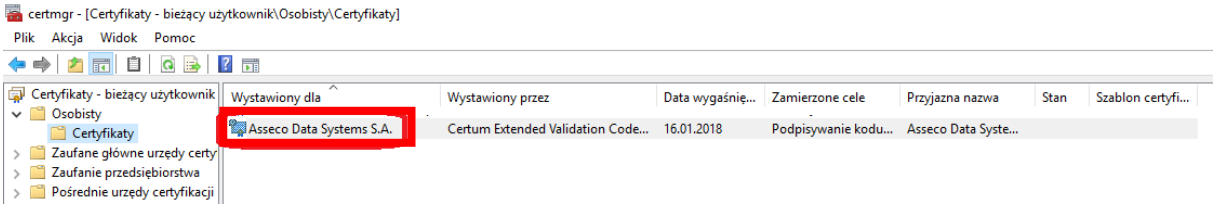
Signtool to narzędzie wiersza polecenia, które cyfrowo **podpisuje pliki**, **weryfikuje podpisy** w plikach i **oznacza pliki znacznikami czasu**. Narzędzie to znaleźć można w paczce deweloperskiej Windows (Windows SDK[Software Development Kit]). Wszystkie operacje wykonywane z Code Signing wymagają podłączonego czytnika wraz z kartą na której jest certyfikat Code Signing. Szerszy opis narzędzia można znaleźć pod adresem: https://msdn.microsoft.com/pl-pl/library/8s9b9yaz(v=vs.110).aspx

5.2 Podpisywanie

Aby podpisać plik, w wierszu poleceń(cmd.exe) należy użyć następującego polecenia:
signtool sign /n "[1] " / t [2] /fd [3] /v [4]

[1] – Nazwa właściciela certyfikatu, którą sprawdzić można w aplikacji proCertum CardManager lub narzędziu systemowym certmgr.msc





[2] – Adres znacznika czasu. Dla Certum http://time.certum.pl,
[3] – Nazwa algorytmu podpisu. Dostępne sha1 i sha256,
[4] – Ścieżka do pliku podpisywanego.

Przykładowe, poprawne polecenie:

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

2.2 Weryfikacja

Aby zweryfikować plik, w wierszu poleceń(cmd.exe) należy użyć następującego polecenia:
signtool verify /pa [1]

[1] – Nazwa podpisanego pliku

Przykładowe, poprawne polecenie:

> **signtool verify /pa file.exe**

3 Jarsigner

3.1 Opis narzędzia

Jarsigner to narzędzie wiersza poleceń, które cyfrowo **podpisuje pliki** oraz **weryfikuje podpisy.** Narzędzie to znaleźć można w paczce deweloperskiej Oracle(JDK [Java Development Kit]). Wszystkie operacje wykonywane z Code Signing wymagają podłączonego czytnika wraz z kartą na której jest certyfikat. Szerszy opis narzędzia można znaleźć pod adresem:
http://docs.oracle.com/javase/7/docs/technotes/tools/windows/jarsigner.html

3.2 Konfiguracja

Przed rozpoczęciem używania *jarsigner* potrzebna jest dodatkowa konfiguracja. 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]**
> **slot=[3]**

[1] – Nazwa providera. Najlepiej Crypto3PKCS.
[2] – Ścieżka do biblioteki PKCS. Jeżeli posiadamy zainstalowanego proCertum CardManagera ścieżka domyślna to: *C:\Windows\System32\crypto3PKCS.dll*
[3] – Numer slota w którym znajduje się karta. Domyślna wartość to -1 która powoduje automatyczne wykrycie pierwszego dostępnego slotu.

Przykładowa konfiguracja:

name=Crypto3CSP
library=C:\Windows\System32\crypto3PKCS.dll
slot=-1

3.3 Podpisywanie

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

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

[1] – Adres znacznika czasu. Dla Certum http://time.certum.pl,
[2] – Ścieżka do pliku konfiguracyjnego providera(Sekcja „Konfiguracja”),
[3] – Hasło do karty,
[4] – Ścieżka do pliku podpisywanego,
[5] – Nazwa właściciela certyfikatu który sprawdzić można w proCertum CardManagerze.

Przykładowe, poprawne polecenie:

jarsigner -keystore NONE -tsa "http://time.certum.pl" -storetype PKCS11 -providerClass sun.security.pkcs11.SunPKCS11 -providerArg "provider.cfg" -storepass "123456" "[signed]proCertumJavaApi.jar" "Asseco Data Systems S.A."

3.4 Weryfikacja

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

jarsigner -verify -verbose -keystore NONE -tsa "[1]" -storetype PKCS11 -providerClass sun.security.pkcs11.SunPKCS11 -providerArg "[2] " -storepass "[3]" "[4]" "[5]"

[1] – Adres znacznika czasu. Dla Certum http://time.certum.pl,
[2] – Ścieżka do pliku konfiguracyjnego providera(Sekcja „Konfiguracja”),
[3] – Hasło do karty,
[4] – Ścieżka do pliku podpisywanego,
[5] – Nazwa właściciela certyfikatu który sprawdzić można w proCertum CardManagerze.

Przykładowe, poprawne polecenie:

jarsigner -verify -verbose -keystore NONE -tsa "http://time.certum.pl" -storetype PKCS11 -providerClass sun.security.pkcs11.SunPKCS11 -providerArg "provider.cfg" -storepass "123456" "[signed]proCertumJavaApi.jar" "Asseco Data Systems S.A."