

UNIZETO



POWSZECHNE  
CENTRUM CERTYFIKACJI



instrukcja użytkownika

# Standard Code Signing

Użycie certyfikatów do podpisywania  
kodu w technologii Java

wersja 1.3

# Spis treści

|  |           |
|--|-----------|
| <b>WSTĘP .....</b>   | <b>3</b>  |
| <b>1. TWORZENIE KLUCZA PRYWATNEGO I CERTYFIKATU .....</b>              | <b>3</b>  |
| 1.1. TWORZENIE ŻĄDANIA CERTYFIKATU (CSR).....                          | 3         |
| 1.2. AKTYWACJA CERTYFIKATU.....  | 5         |
| 1.3. WKLEJENIE ŻĄDANIA CSR (ŻĄDANIE WYDANIA CERTYFIKATU) .....         | 6         |
| 1.4. POBIERANIE CERTYFIKATU CERTUM CA I CERTYFIKATÓW POŚREDNICH.....   | 11        |
| 1.5. IMPORTOWANIE CERTYFIKATU CERTUM CA I CERTYFIKATÓW POŚREDNICH..... | 11        |
| 1.6. INSTALOWANIE CERTYFIKATU UŻYTKOWNIKA .....                        | 12        |
| <b>2. PODPISYWANIE KODU .....</b>                                      | <b>14</b> |
| <b>3. WERYFIKOWANIE .....</b>  | <b>15</b> |
| <b>4. IMPORT/EKSPORT KLUCZY.....</b>                                   | <b>15</b> |
| <b>5. SPIS RYSUNKÓW.....</b>   | <b>16</b> |

## Wstęp

Wykonywalny kod Java może być podpisany cyfrowo w technologii *Java Code Signing* przy zastosowaniu specjalnego certyfikatu do podpisywania kodu, oferowanego przez CERTUM. Niezbędna do tego celu jest również aplikacja *Sun JDK* (w szczególności programy *keytool* oraz *jarsigner*, lub dostępny w starszych wersjach *javakey*). Dzięki podpisowi cyfrowemu dowolny aplet lub plugin może żądać rozszerzonych uprawnień. Podpis cyfrowy daje odbiorcy dużą pewność co do autentyczności kodu. W celu uzyskania dalszych informacji odwiedź stronę Sun Java Developer Kit.

## 1. Tworzenie klucza prywatnego i certyfikatu

### 1.1. Tworzenie żądania certyfikatu (CSR)

Zmień katalog na *c:\Program Files\Java\jdk1.x* (lub inny gdzie została zainstalowana Java), gdzie *x* oznacza wersję Javy lub dodaj tą ścieżkę do *PATH* i wydaj polecenie:

```
keytool -genkey -keyalg RSA -keysize 2048 -alias cunizetowski
```

Powyższe polecenie spowoduje wygenerowanie klucza prywatnego wraz z odpowiadającym mu żądaniem certyfikatu CSR. Algorytm generujący klucze jest zgodny ze standardem *RSA* i jest 2048 bitowej długości. *-alias* jest nazwą certyfikatu np. Imię, pseudonim itp.

Podczas generowania CSR będziesz musiał podać poniższe informacje:

- **What is your first and last name ?**

podaj swoje imię i nazwisko, np. Jan Kowalski. W przypadku, kiedy staramy się o certyfikat dla firmy programistycznej powinniśmy podać nazwę firmy lub jej alias, np.: Firma Trusted Code, Firma S.A, Firma Java Code itp.

- **What is the name of your organizational unit ?**

podaj nazwę oddziału lub wydziału swojej firmy czy instytucji, dla której starasz się o certyfikat. Osoby prywatne mogą wpisać: Unizeto(r) Developer Certificates, pozostali podają jednostkę organizacyjną np.: Dział Programowania, Instytut Metalurgii, Oddział Intensywnej Terapii itp.

- **What is the name of your organization ?**

podaj nazwę swojej firmy lub instytucji, dla której starasz się o certyfikat. Osoby prywatne mogą wpisać: Java Code Signing, pozostali podają nazwę firmy lub Organizacji np.: Firma S.A, Uniwersytet w Ludowie Dolnym, Klub Kubusia Puchatka itp.

- **What is the name of your City or Locality ?**

Podaj nazwę swojej miejscowości, np.: Szczecin, Warszawa, Lodowo Dolne itp.

- **What is the name of your State or Province ?**

Podaj nazwę swojego województwa nie stosując skrótów, np.: Zachodniopomorskie, Mazowieckie itd.

**- What is the two-letter country code for this unit ?**

Podaj kod ISO swojego kraju - PL (duże litery). Nie należy stosować małych liter lub innych "popularnych" oznaczeń, np.: RP, PRL itd.

**Uwaga:** Używanie znaków specjalnych % ^ \$ \_ lub polskich znaków diakrytycznych: ŹźćąŁ przy podawaniu tych informacji spowoduje nieprawidłowe wygenerowanie certyfikatu!

Przykład wygenerowania pary kluczy przy użyciu narzędzia *keytool* :

```
C:\j2sdk1.4.1.0_7\bin>keytool -genkey -keyalg RSA -keysize 2048 -alias cunizetowski
Enter keystore password: moje_haslo
What is your first and last name?
  [Unknown]: Certacy Unizetowski
What is the name of your organizational unit?
  [Unknown]: Moja Firma
What is the name of your organization?
  [Unknown]: Oddzial w Moja Firma
What is the name of your City or Locality?
  [Unknown]: Szczecin
What is the name of your State or Province?
  [Unknown]: Zachodniopomorskie
What is the two-letter country code for this unit?
  [Unknown]: PL
Is CN=Certacy Unizetowski, OU=Moja Firma, O=Oddzial w Moja Firma, L=Szczecin, ST
=Zachodniopomorskie, C=PL correct?
[no]: yes

Enter key password for <cunizetowski>
  (RETURN if same as keystore password):

C:\j2sdk1.4.1.0_7\bin>
```

Aby sprawdzić czy polecenie zostało wykonane poprawnie, można użyć polecenia *keytool -list* lub *keytool -list -v*. Obie te opcje wyświetlą (z różnym poziomem szczegółowości) zawartość bazy z kluczami *./keystore*:

```
C:\j2sdk1.4.1_07\bin>keytool -list -keystore "c:\Documents and Settings\Administrator\keystore"
Enter keystore password: moje_haslo

Keystore type: jks
Keystore provider: SUN

Your keystore contains 1 entry

cunizetowski, 2005-07-22, keyEntry,
Certificate fingerprint (MD5): 8B:8B:CA:1C:50:AA:D7:A8:75:C1:84:27:D9:6D:EA:BB

C:\j2sdk1.4.1_07\bin>
```

Po wykonaniu powyższej czynności należy wydać polecenie:

```
keytool -certreq -alias cunizetowski -file c:\mycert.csr
```

Spowoduje to zapisanie żądania certyfikatu o nazwie *cunizetowski* do pliku *mycert.csr* :

```
C:\j2sdk1.4.1_07\bin>keytool -certreq -alias cunizetowski -file c:\mycert.csr
Enter keystore password: moje_haslo

C:\j2sdk1.4.1_07\bin>_
```

Przykładowy plik żądania powinien wyglądać podobnie jak poniżej:

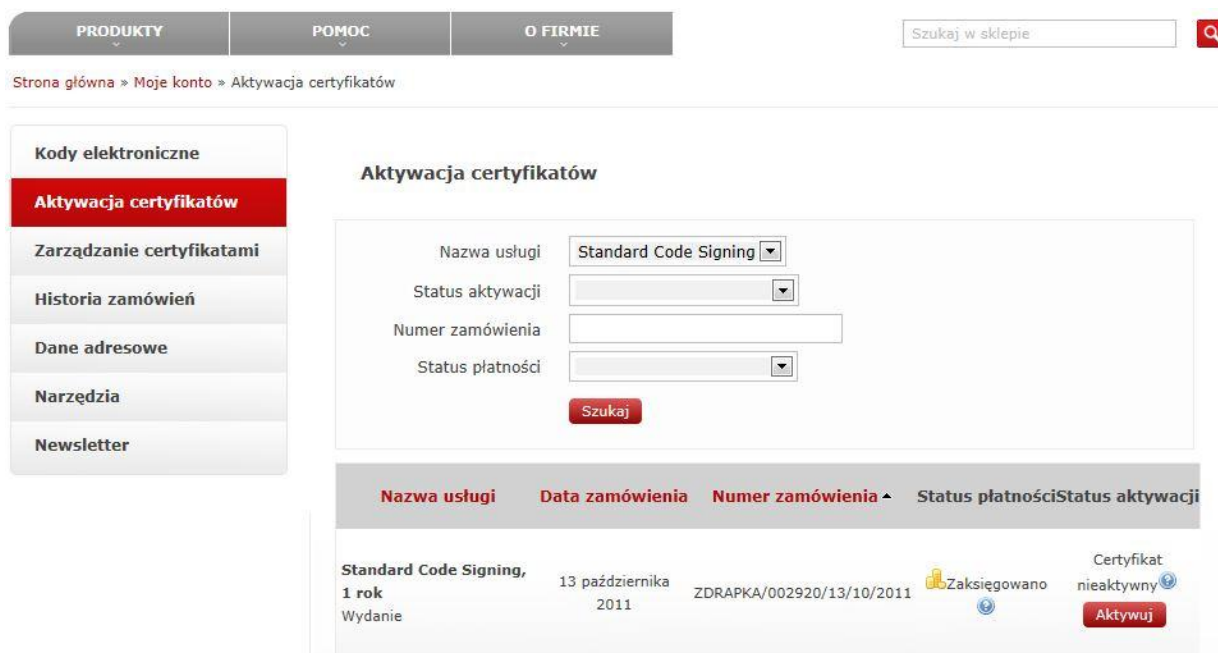


```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIB0DCCATkCAQAwgY8xCZAJBgNVBAYTA1BMMRswGQYDVQQLIE1JYWNob2Ruaw9wb21vcnNr
aWUXETAPBgNVBAClTCFN6Y3p1Y21uMR0wGwYDVQKEXRlZGR6aWFSIHcgTW9qYSBGaXJt
YU9w0B
CxMKTW9qYSBGaXJtYU9w0BGA1UEAxMTQ2vydGFjeSBVbm16ZXRvd3NraTCBnzANBgkq
hkiG9w0B
AQEFAA0BjQAwgYkCgYEAoHaZBVXkMZ+A3DPrSwWZz5QZVH2Tmy35QvZS7E3ScNHLs0
1rECy+aLwT
+mnGLbTlX3PUi4YcgCKsJTeu/mwCkmIDGAIeumHowPcdNZH7dEdM0AggIpaNqMivl
JkyQJdnF9Y
G92gzEnKIXyysx7C9Ipb7ItI1V39EF40eiGFNmsCAwEAAaAAMA0GCSqGSIb3DQEB
BAUAA4GBAALp
xIgz2rCTIVq8K8DgPCPiufJ4lJUvw1jvk4nmH5iqueMayIDpbTEwwX5s12dwqyF/
+Z3MguwxIAKY
gHJN4x/jns90ozsmIGUE6sANVKF93CrM+n17dcd1HgMzrGv5xnt+H2z0JhiBOVjd5gs
1v8orEI1h
S1DDMQwDB6Xs0xb+
-----END NEW CERTIFICATE REQUEST-----
```

## 1.2. Aktywacja certyfikatu

15. Po zaksięgowaniu wpłaty przez firmę Unizeto Technologies SA otrzymasz e-mail z powiadomieniem o zaksięgowaniu płatności i dostępnym kodzie aktywacyjnym, który umożliwi wygenerowanie żądania o uzyskanie certyfikatu.

16. Logujemy się na swoje konto w e-sklepie (<https://sklep.unizeto.pl>). Przechodzimy do zakładki **Aktywacja Certyfikatów**.



Rysunek 1 – Aktywacja certyfikatu Standard Code Signing

### 1.3. Wklejenie żądania CSR (żądanie wydania certyfikatu)

Ze względu na specyfikację certyfikatu **do podpisywania kodu JAVA** wybieramy metodę **CSR** (żądanie podpisania certyfikatu, które zostało utworzone wcześniej patrz rozdział 1.1 ) i postępujemy zgodnie z instrukcjami przedstawionymi w dalszej części instrukcji.

1. Wybieramy metodę CSR i klikamy **Dalej**.

The screenshot shows the 'Aktywacja' (Activation) page in the CERTUM system. The page is part of a multi-step process: 1. Zamówienia, 2. Wybór metody (selected), 3. Klucze, 4. Dane, 5. Potwierdzenie. The service being activated is 'Standard Code Signing, 1 rok' with the type 'Wydanie'. Under 'Wybierz sposób dostarczenia kluczy dla certyfikatu', the 'CSR' option is selected. A 'Dalej >>' button is visible at the bottom of the main content area.

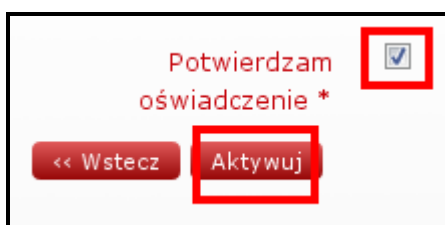
**Rysunek 2 – CSR wybór metody**

2. W ramkę należy wkleić wcześniej wygenerowane żądanie CSR.



**Uwaga:** Prosimy o dokładną weryfikację danych do certyfikatu. Po dokonaniu aktywacji usługi, zmiana danych nie będzie możliwa. Zanim złożysz wniosek o wydanie certyfikatu, potwierdzisz go, bądź użyjesz do realizacji pierwszego podpisu powinieneś dokładnie przeczytać tekst oświadczenia zawartego na stronie. Jeśli nie zgadzasz się z warunkami niniejszego oświadczenia, nie składaj wniosku o wydanie certyfikatu.

Jeżeli zapoznaliśmy się z zawartością oświadczenia, **zaznaczamy checkbox** i wybieramy przycisk **Aktywuj**.



**Rysunek 5 – Potwierdzenie oświadczenia Cz. 1**

**Kody elektroniczne**  
**Aktywacja certyfikatów**  
Zarządzanie certyfikatami  
Historia zamówień  
Dane adresowe  
Narzędzia  
Newsletter

**Aktywacja**

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

Nazwa usługi: **Standard Code Signing, 1 rok**  
Wydanie

**Dane do certyfikatu:**

|                               |                         |
|-------------------------------|-------------------------|
| Nazwa                         | Adam Nowak              |
| Początek ważności certyfikatu | 19 października 2011    |
| Koniec ważności certyfikatu   | 18 października 2012    |
| Organizacja                   | Unizeto Technologies SA |
| Jednostka organizacyjna       | Unizeto Technologies SA |
| Kraj                          | Polska                  |
| Email                         | adam.nowak@unizeto.pl   |

**Prosimy o dokładną weryfikację danych do certyfikatu. Po dokonaniu aktywacji usługi, zmiana danych nie będzie możliwa.**

**Struktura certyfikatu:**

Podmiot: E=adam.nowak@unizeto.pl, CN=Adam Nowak, OU=Unizeto Technologies SA, O=Unizeto Technologies SA, C=PL

**Oświadczenie**

Centrum Certyfikacji. Przedkładając wniosek o wydanie certyfikatu żądasz od organu je wydającego rozpatrzenia i wydania certyfikatu; jednocześnie oświadczasz, że akceptujesz warunki w nim określone.

Usługi certyfikacyjne świadczone są zgodnie z zasadami określonymi w Kodeksie Postępowania Certyfikacyjnego (KPC), który przez przywołanie staje się integralną częścią niniejszego oświadczenia. Kodeks Postępowania Certyfikacyjnego dostępny jest poprzez internet w repozytorium CERTUM - Powszechne Centrum Certyfikacji pod adresem <http://www.certum.pl/repozytorium/> lub za pośrednictwem poczty elektronicznej na wniosek wysłany na adres [info@certum.pl](mailto:info@certum.pl).

Czynności prawne dokonane z użyciem niniejszego certyfikatu nie wywołują na terenie Rzeczypospolitej Polskiej skutków prawnych, równorzędnych podpisowi własnoręcznemu.

Potwierdzam oświadczenie \*

<< Wstecz Aktywuj

**Rysunek 6 – Potwierdzenie oświadczenia Cz. 2**

4. Na tym etapie użytkownik otrzyma informacje na adres:

**Wniosek certyfikacyjny został utworzony** - Przy zakupie certyfikatu **Standard Code Signing** wymagana jest weryfikacja tożsamości przyszłego Subskrybenta. Nowi klienci proszeni są o dostarczenie w terminie do 7 dni kopii dokumentów (lista wymaganych dokumentów będzie podana w otrzymanym e-mailu),

**Temat:** Wniosek certyfikacyjny został utworzony

Szanowni Państwo,

Dziękujemy za złożenie zamówienia na certyfikat **Standard Code Signing** dla **Firmy**. Wniosek o wydanie certyfikatu został wstępnie rozpatrzony.

Przy zakupie certyfikatu **Standard Code Signing** wymagana jest weryfikacja tożsamości przyszłego Subskrybenta. Prosimy o dostarczenie w terminie 7 dni kopii następujących dokumentów:

**Dokumenty wymagane od osoby prywatnej:**

- kopia dokumentu na podstawie którego będzie można potwierdzić tożsamość osoby odpowiedzialnej za zakup certyfikatu (**dowód tożsamości, paszport, karta stałego pobytu, prawo jazdy**).

**Dokumenty wymagane od osoby reprezentującej organizację:**

- kopia dokumentu na podstawie którego będzie można potwierdzić tożsamość osoby odpowiedzialnej za zakup certyfikatu (**dowód tożsamości, paszport, karta stałego pobytu, prawo jazdy**),
- dokument potwierdzający związek osoby zamawiającej certyfikat z firmą (chyba, że powiązanie wykazane jest np. w KRS-ie) – świadectwo **zatrudnienia lub upoważnienie**,
- dokumenty firmy – **akt nadania numeru NIP lub REGON**,

Wszystkie zebrane dokumenty prosimy wysłać do CERTUM PCC na jeden z poniższych sposobów:

- a) e-mailem w formie skanu na adres: [ccp@certum.pl](mailto:ccp@certum.pl) (forma zalecana)
- b) faxem na numer fax: +48 (0) 91 4257 422
- c) pocztą na adres:

CERTUM PCC  
ul. Bajeczna 13  
71-838 Szczecin

W przypadku jakichkolwiek pytań prosimy o kontakt z Operatorem naszej Infolinii:

- e-mail: [infolinia@unizeto.pl](mailto:infolinia@unizeto.pl)

- nr tel.: 801 540 340 (czynna 24h na dobę),
- dla telefonów komórkowych +48 91 4801 340 (czynna 24h na dobę),

Z poważaniem

Zespół CERTUM PCC

5. Bezpośrednio po złożeniu wniosku status wniosku przedstawiany jest jako **Oczekuje na realizację**. Po zweryfikowaniu wymaganych dokumentów i zaakceptowaniu wniosku przez **Centrum Certyfikacji** status wniosku zmieni się na **Zaakceptowany** i następnie zmieni się automatycznie na **W trakcie realizacji**.

Po wydaniu certyfikatu status wniosku zmieni się automatycznie na **Wydany**. Wniosek zostanie wtedy usunięty z listy wniosków, a użytkownik, który złożył wniosek będzie mógł zainstalować certyfikat wg opisu przedstawionego w rozdziale opisującym tę czynność.

6. Po dosłaniu dokumentów formalnych użytkownik otrzymuje na adres e-mail z informacją o wydaniu certyfikatu.

**Temat:** Certyfikat został utworzony.

Szanowni Państwo,

Certyfikat **Standard Code Signing** o numerze seryjnym **2475491978e7fd4ceba932f2269b6a9** dla **Unizeto Technologies SA** został właśnie wydany.

Okres ważności certyfikatu: od: **19.10.2011** do: **18.10.2012**.

Instalacji certyfikatu można dokonać za pośrednictwem konta klienta w systemie CERTUM PCC.

<https://cservices.certum.pl/muc-customer/partner/customerCertificate/view?themeId=default&linkId=KxKcZXC%2FGt656TltMf1KFrwxEMg%3D%0D%0A>

W przypadku jakichkolwiek pytań prosimy o kontakt z Operatorem naszej Infolinii:

- e-mail: [infolinia@unizeto.pl](mailto:infolinia@unizeto.pl)
- nr tel.: 801 540 340 (czynna 24h na dobę),
- dla telefonów komórkowych +48 91 4801 340

Z poważaniem

Zespół Certum PCC

7. Pobranie certyfikatu można dokonać za pośrednictwem konta klienta w systemie CERTUM PCC.

#### 1.4. Pobieranie certyfikatu Certum CA i certyfikatów pośrednich

Aby pobrać certyfikat Certum CA lub certyfikaty pośrednie należy wejść na stronę [www.certum.pl](http://www.certum.pl) do działu *Obsługa certyfikatów* → *Zaświadczenia i klucze*. Po wybraniu certyfikatu należy wybrać opcję *Certyfikat dla serwerów WWW*.

| Główny klucz urzędu - Certum CA           |   |
|---|---|
| Nr seryjny:                               | 10020                                   |
| Ważny od:                                 | Jun 11 10:46:39 2002 GMT                |
| Ważny do:                                 | Jun 11 10:46:39 2027 GMT                |
| Certyfikat dla Przeglądarek Internetowych | <input type="button" value="Instaluj"/> |
| Certyfikat dla Serwerów WWW i SSL/TLS     | <input type="button" value="Instaluj"/> |
| Certyfikat dla urządzeń sieciowych        | <input type="button" value="Instaluj"/> |

[do góry ↗](#)

Wyświetli się interesujący nas certyfikat, który zaznaczymy myszką, wkleimy do pliku i zapiszemy.

**UWAGA:** W celu wklejania do pliku certyfikatu prezentowanego na stronie należy skopiować fragment tekstu od linii "--BEGIN CERTIFICATE --" do "--END CERTIFICATE--", używając do tego celu edytora tekstowego np. Notepad i myszki. **Nie należy używać do tej operacji Worda, czy innego procesora tekstowego!**

W przypadku pobierania certyfikatów pośrednich, wybieramy interesujący nas certyfikat, np. CERTUM Level IV z listy (Certyfikaty Level IV należy pobrać w przypadku, gdy posiadamy certyfikat typu Trusted, certyfikat poziomu III należy pobrać w sytuacji, gdy posiadamy certyfikat typu Enterprise / Wildcard, certyfikat poziomu II należy pobrać w sytuacji, gdy posiadamy certyfikat typu Commercial; dla certyfikatów typu Private pobierany jest certyfikat klasy I). Pozostała część procesu (zapisanie do pliku) przebiega jak dla certyfikatu Certum CA.

#### 1.5. Importowanie certyfikatu Certum CA i certyfikatów pośrednich

Aby do bazy certyfikatów dodać certyfikat Certum CA należy wydać polecenie:

```
keytool -import -trustcacerts -file c:\work\CA.der -alias CertumCA
```

W ten sposób do bazy z zaufanymi urzędami certyfikującymi zostanie dodany certyfikat Certum CA. Opcja `-file` wskazuje nam położenie pliku z certyfikatem, z kolei `-alias` to nazwa, pod którą certyfikat będzie widniał w bazie:

```
C:\j2sdk1.4.1_07\bin>keytool -import -trustcacerts -file C:\work\CA.der -alias CertumCA
Enter keystore password: moje_haslo
Owner: CN=Certum CA, O=Unizeto Sp. z o.o., C=PL
Issuer: CN=Certum CA, O=Unizeto Sp. z o.o., C=PL
Serial number: 10020
Valid from: Tue Jun 11 12:46:39 CEST 2002 until: Fri Jun 11 12:46:39 CEST 2027
Certificate fingerprints:
    MD5: 2C:8F:9F:66:1D:18:90:B1:47:26:9D:8E:86:82:8C:A9
    SHA1: 62:52:DC:40:F7:11:43:A2:2F:DE:9E:F7:34:8E:06:42:51:B1:81:18
Trust this certificate? [no]: yes
Certificate was added to keystore
```

```
C:\j2sdk1.4.1_07\bin>
```

Procedurę powtarzamy dla certyfikatu pośredniego, używając polecenia:

```
keytool -import -trustcacerts -file c:\work\CA1.der -alias Certumlvl_1
```

Do bazy zostanie dodany certyfikat pośredni Certum Level I. Znaczenie opcji *-file* i *-alias* jest takie same jak powyżej.

```
C:\j2sdk1.4.1_07\bin>keytool -import -trustcacerts -file C:\work\CA1.der -alias Certumlevel_1
Enter keystore password: moje_haslo
Certificate was added to keystore
```

Aby wyświetlić zawartość naszej bazy z certyfikatami użyjemy opcji:

```
keytool -list
```

lub

```
keytool -list -v
```

```
C:\j2sdk1.4.1_07\bin>keytool -list
Enter keystore password: moje_haslo
```

```
Keystore type: jks
Keystore provider: SUN
```

```
Your keystore contains 3 entries
```

```
certumca, 2005-07-22, trustedCertEntry,
Certificate fingerprint (MD5): 2C:8F:9F:66:1D:18:90:B1:47:26:9D:8E:86:82:8C:A9
certumlevel_1, 2005-07-22, trustedCertEntry,
Certificate fingerprint (MD5): A1:42:3D:0A:27:16:ED:DC:2E:94:81:29:D6:3B:98:52
cunizetowski, 2005-07-22, keyEntry,
Certificate fingerprint (MD5): 9F:67:DB:A3:83:49:E6:73:E9:7C:BE:61:EE:91:8F:89
```

```
C:\j2sdk1.4.1_07\bin>_
```

## 1.6. Instalowanie certyfikatu użytkownika

1. Pobranie certyfikatu można dokonać za pośrednictwem konta klienta w systemie CERTUM PCC. Wchodzimy na stronę <https://sklep.unizeto.pl/> → zakładka **Zarządzanie certyfikatami**

PRODUKTY    POMÓC    O FIRMIE

Szukaj w sklepie

Strona główna » Moje konto » Zarządzanie certyfikatami

Kody elektroniczne

Aktywacja certyfikatów

**Zarządzanie certyfikatami**

Historia zamówień

Dane adresowe

Narzędzia

Newsletter

### Zarządzanie certyfikatami

**Profil certyfikatu**     **Status**

**Nazwa**      Ważny

**Email**      Unieważniony

**Wydany po**      Wygasły

**Wydany przed**      Uzyska ważność

**Szukaj**

| Nr seryjny                               | Profil certyfikatu       | Email                        | Nazwa                         | Ważny od                              | Ważny do                              | Status                                    |
|--|--------------------------|------------------------------|-------------------------------|---------------------------------------|---------------------------------------|---|
| 2475491978e7f<br>d4cehaf932f22<br>69b6a9 | Standard Code<br>Signing | marcin.sztyrbicki@unizeto.pl | Unizeto<br>Technologies<br>SA | 19<br>październik<br>2011<br>13:56:03 | 18<br>październik<br>2012<br>13:56:03 | <input checked="" type="checkbox"/> Ważny |

Rysunek 7 – Profil certyfikatu Java Code Signing

2. Aby pobrać certyfikat wybieramy przycisk **Zapisz binarnie**.

Kody elektroniczne

Aktywacja certyfikatów

**Zarządzanie certyfikatami**

Historia zamówień

Dane adresowe

Narzędzia

Newsletter

### Zarządzanie certyfikatami

**Profil certyfikatu**     **Status**

**Nazwa**      Ważny

**Email**      Unieważniony

**Wydany po**      Wygasły

**Wydany przed**      Uzyska ważność

**Szukaj**

| Nr seryjny                               | Profil certyfikatu       | Email                        | Nazwa                         | Ważny od                              | Ważny do                              | Status                                    |
|--|--------------------------|------------------------------|-------------------------------|---------------------------------------|---------------------------------------|---|
| 2475491978e7f<br>d4cehaf932f22<br>69b6a9 | Standard Code<br>Signing | marcin.sztyrbicki@unizeto.pl | Unizeto<br>Technologies<br>SA | 19<br>październik<br>2011<br>13:56:03 | 18<br>październik<br>2012<br>13:56:03 | <input checked="" type="checkbox"/> Ważny |

**Nazwa** Unizeto Technologies SA

**Organizacja** Unizeto Technologies SA

**Jednostka organizacyjna** Unizeto Technologies SA

**Email** marcin.sztyrbicki@unizeto.pl

Rysunek 8 – Zapis w postaci binarnej certyfikatu Java Code Signing

Zapisywany plik certyfikatu powinien być szyfrowany binarnie algorytmem DER – ściągnij certyfikat z naszej strony poprzez Zapisz binarnie zapisujemy certyfikat szyfrowany algorytmem DER – rozszerzenie \*.cer, a następnie należy wydać polecenie (nie ma konieczności zmiany rozszerzenia z \*.cer na \*.der):

```
keytool -import -file c:\work\certkod.der -alias cunizetowski
```

**gdzie:** -alias oznacza nazwę certyfikatu, natomiast -file jest ścieżką prowadzącą do naszego pliku z certyfikatem:

```
C:\j2sdk1.4.1_07\bin>keytool -import -file c:\work\certkod.der -alias cunizetowski
Enter keystore password: moje_haslo
Certificate was added to keystore
```

```
C:\j2sdk1.4.1_07\bin>
```

Aby wyświetlić zawartość naszej bazy z certyfikatami użyjemy opcji:

```
keytool -list
```

lub

```
keytool -list -v
```

```
C:\j2sdk1.4.1_07\bin>keytool -list
Enter keystore password: moje_haslo
```

```
Keystore type: jks
Keystore provider: SUN
```

```
Your keystore contains 3 entries
```

```
certumca, 2005-07-22, trustedCertEntry,
Certificate fingerprint (MD5): 2C:8F:9F:66:1D:18:90:B1:47:26:9D:8E:86:82:8C:A9
certumlevel_1, 2005-07-22, trustedCertEntry,
Certificate fingerprint (MD5): A1:42:3D:0A:27:16:ED:DC:2E:94:81:29:D6:3B:98:52
cunizetowski, 2005-07-22, keyEntry,
Certificate fingerprint (MD5): 9F:67:DB:A3:83:49:E6:73:E9:7C:BE:61:EE:91:8F:89
```

```
C:\j2sdk1.4.1_07\bin>_
```

## 2. Podpisywanie kodu

Przejdź do katalogu, w którym zapisany jest program *jarsigner* (domyślnie *c:\Program Files\Java\jdk1.x.o\bin\*, gdzie x oznacza numer wersji javy - można również dodać ścieżkę do PATH) i wydaj polecenie:

```
jarsigner Notepad.jar cunizetowski
```

Spowoduje to złożenie podpisu na pliku *Notepad.jar* przy użyciu klucza o nazwie *cunizetowski*:

```
C:\work\jar>jarsigner Notepad.jar cunizetowski
Enter Passphrase for keystore: moje_haslo
```

```
C:\work\jar>
```

### 3. Weryfikowanie

Aby zweryfikować poprawność podpisu wydajemy polecenie:

```
C:\work\jar>jarsigner -verify Notepad.jar  
jar verified.
```

```
C:\work\jar>_
```

W celu uzyskania bardziej szczegółowych informacji o podpisie, wpisujemy:

```
C:\work\jar>jarsigner -verify -verbose -certs Notepad.jar
```

Wyświetlone zostaną szczegółowe dane podpisów.

```
smk      20348 Sat Dec 06 19:57:34 CET 2003 src/Notepad.java  
X.509, CN=Certacy Unizetowski, O=Oddzial w Moja Firma, C=PL (cunizetowski)  
X.509, CN=Certum Level I, O=Unizeto Sp. z o.o., C=PL (certumlevel_1)  
X.509, CN=Certum CA, O=Unizeto Sp. z o.o., C=PL (certumca)  
X.509, CN=Certacy Unizetowski, OU=Moja Firma, O=Oddzial w Moja Firma,  
L=Szczecin, ST=Zachodniopomorskie, C=PL  
  
s = signature was verified  
m = entry is listed in manifest  
k = at least one certificate was found in keystore  
i = at least one certificate was found in identity scope  
jar verified.
```

### 4. Import/Eksport kluczy

Po otrzymaniu certyfikatu wskazane jest by klucz prywatny zabezpieczony został na osobnym nośniku, np. dyskietce lub CD. Wszystkie niezbędne do pracy programu klucze dla podpisywania apletów Java przechowywane są w pliku \*.keystore (w katalogu domowym). Jego zabezpieczenie pozwala odzyskać certyfikat w wypadku awarii dysku twardego.

## 5. Spis rysunków

|  |    |
|--|----|
| Rysunek 1 – Aktywacja certyfikatu Standard Code Signing .....            | 5  |
| Rysunek 2 – CSR wybór metody .....                                       | 6  |
| Rysunek 3 – Wklejenie żądania CSR .....                                  | 7  |
| Rysunek 4 – Dane do certyfikatu .....                                    | 7  |
| Rysunek 5 – Potwierdzenie oświadczenia Cz. 1 .....                       | 8  |
| Rysunek 6 – Potwierdzenie oświadczenia Cz. 2 .....                       | 8  |
| Rysunek 7 – Profil certyfikatu Java Code Signing .....                   | 13 |
| Rysunek 8 – Zapis w postaci binarnej certyfikatu Java Code Signing ..... | 13 |