

UNIZETO



POWSZECHNE
CENTRUM CERTYFIKACJI



instrukcja użytkownika

Tomcat + SSL - Windows/Linux

Instalacja certyfikatów niekwalifikowanych
w serwerze Tomcat

wersja 1.0

Spis treści

1. WSTĘP.....	3
2. GENEROWANIE CERTYFIKATU	3
2.1. GENEROWANIE PARY KLUCZY RSA	3
2.2. GENEROWANIE ŻĄDANIA WYDANIA CERTYFIKATU.....	4
2.3. TWORZENIE CERTYFIKATU NA PODSTAWIE WYSŁANEGO ŻĄDANIA	5
3. INSTALACJA CERTYFIKATU I KLUCZA PRYWATNEGO.....	7
3.1. EKSPORT KLUCZA PRYWATNEGO DO FORMATU PKCS12	7
3.2. ZMIANA KONFIGURACJI SERWERA TOCCAT	9
4. UWIERZYTELNIANIE UŻYTKOWNIKÓW NA PODSTAWIE CERTYFIKATÓW KLUCZA PUBLICZNEGO.....	10
4.1. INSTALACJA CERTYFIKATÓW URZĘDU CERTYFIKACJI CERTUM CA	10
4.2. EDYCJA PLIKÓW KONFIGURACYJNYCH.....	11
4.3. PLIK SERVER.XML.....	11
4.4. PLIK TOMCAT-USERS.XML	11
4.5. PLIK WEB.XML.....	12

1. Wstęp

Tomcat jest serwerem implementującym technologię JavaServlet i JavaServer Pages. Jest dostępny zarówno dla systemu Linux jak i dla Windows. Opublikowany na licencji Apache Software License jest dobrą platformą do obsługi aplikacji Java w sieci. Tomcat ma wbudowane wsparcie dla silnej kryptografii.

W tej instrukcji opisano jak skonfigurować serwer Tomcat w systemie Windows. Konfiguracja w systemie Linux jest podobna do konfiguracji w Windows. Zmianie ulegają jedynie ścieżki do katalogów. Pliki konfiguracyjne znajdują się w katalogu `/etc/tomcat5.5` (zależnie od wersji serwera nazwa katalogu może się nieznacznie różnić).

Należy utworzyć katalog, w którym zostaną umieszczone certyfikaty i klucz prywatny serwera. Wskazane jest nadanie odpowiednich uprawnień (o ile nie zrobił tego menedżer pakietów bądź instalator):

```
chmod 750 /etc/tomcat5.5
```

Aby skonfigurować serwer Tomcat ze wsparciem dla silnej kryptografii potrzebne będą następujące elementy:

- Apache Tomcat (<http://tomcat.apache.org/>),
- OpenSSL (<http://www.openssl.org/>, wersja dla systemu Microsoft Windows znajduje się pod adresem: <http://www.slproweb.com/products/Win32OpenSSL.html>).

2. Generowanie certyfikatu

2.1. Generowanie pary kluczy RSA

W wierszu polecenia wydajemy następujące polecenie:

```
OpenSSL> genrsa -aes256 -out server.key 2048
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....+++++
.+++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
OpenSSL>
```

Spowoduje to wygenerowanie pary kluczy RSA i zaszyfrowanie ich algorytmem AES. W czasie generowania pary kluczy należy podać hasło chroniące klucze.

2.2. Generowanie żądania wydania certyfikatu

Kolejnym krokiem będzie wygenerowanie żądania wystawienia certyfikatu. Zostanie użyty klucz wygenerowany w poprzednim kroku. Żądanie wystawienia certyfikatu zostanie zapisane w pliku server.csr. Należy wydać polecenie:

```
OpenSSL> req -new -key server.key -out server.csr
```

Konieczne będzie podanie hasła chroniącego parę kluczy RSA:

```
Enter pass phrase for server.key:
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
```

Następnie należy podać informacje o firmie i domenie:

- Country (C) - dwuliterowy symbol kraju (PL). Należy użyć kodu ISO, np. poprawnym kodem Polski jest
- PL (duże litery), a nie pl czy RP.
- State / Province (ST) - nazwa województwa, np.: Zachodniopomorskie. Nie należy stosować skrótów.
- Locality (L) - nazwa miasta lub wsi, np.: Szczecin, Kozia Wolka, Warszawa.
- Common Name – należy podać nazwę domeny pod jaką widoczna jest strona. W przypadku żądania certyfikatu Wildcard należy dodać przed nazwą domeny „*.”. Ostatecznie to pole powinno wyglądać następująco: *.serwermojefirmy.pl

```
Country Name (2 letter code) [AU]:PL
State or Province Name (full name) [Some-State]:Zachodniopomorskie
Locality Name (eg, city) []:Szczecin
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Moja Firma
Organizational Unit Name (eg, section) []:Odzial Mojej Firmy
Common Name (eg, YOUR name) []:serwermojefirmy.pl
Email Address []:jmila@certum.pl
```

```
Please enter the following 'extra' attributes
to be sent with your certificate request
```

```
A challenge password []:
```

```
An optional company name []:
```

2.3. Tworzenie certyfikatu na podstawie wysłanego żądania

Utworzone żądanie certyfikatu powinno mieć wygląd podobny do przedstawionego przykładu:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC9DCCAdwCAQAwga4xCzAJBgNVBAYTA1BMMRswGQYDVQQIEExJaYWNob2RuaW9w
b21vcnNraWUxETAPBgNVBACITCFN6Y3plY2luMRMwEQYDVQQKEwpNb2phIGZpcmlh
MRwwGgYDVQQLEExNPZGR6aWFsIE1vamVqIEZpcml5MRwwGgYDVQQDEExNzZXJ3ZXJt
b2plamZpcml5LnBsMR4wHAYJKoZIhvcNAQkBFg9qbWlsYUBjZXJ0dW0ucGwwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQNGL2zNP/BfthiuqS5Wop+9ld5
10nR5qsoimxwaOyidk jwNxmAX9YbYjz+fCgDIMuB79X3yMy5c/JnsQSlrSXdtAXT
LOk+uTJQMz6P/sI/SRf9UxsZtfkVtiA6mhWekkOPXfov1BGueJFI+KQj9M/bCyeH
RDX+gUDrFMpSsHroJQ7UW0ZQn8W+FWK06iBceRL5VqazF8631HPaVGqIzHQIu jFU
hIZBodMq7SE5LnUypYJ71RXcGQV1S3VrifESncFZiaEmIFoNPiP8unU4+5xi jPi8
0DGXchmFRKrvL57uwMxnSLDGFuQRyR89/T96fE0nXQBAMHPFipTJskpAvRUNAgMB
AAGgADANBqkqhkiG9w0BAQUFAAOCAQEABBYDA+aShTvrG7Jnnue7NNWz1EQe62+3
ERiPA711ZiOwu/LBFM2c7C9HFxpMlgzv9FwWed2C/4gChrsYTgLLnlmJ0ixDhuP
a0Ck7yxvTgA9KnUTRY+H911D8yriQ2BDD/KUPyQ79v+XnRQWpEjUWCnn/jkqRcSJ
GRKjv2iMORjUmGJNBLa7H8zSJM1N47iK536NNS0W5rXxrRU81gPbDJzPAbR4zgnV
ASBXTWcpPkzLbHxmpTFut8thffagWtqmHgTbbhAOC6lqitlfxE2jzi4AwEFd3tY7
6pYbM9wrj1Cjmwv7PB/oZmGV5A07vKfHxbW93pVlc7ggQXVlyePIZg==
-----END CERTIFICATE REQUEST-----
```

Dysponując gotowym żądaniem wystawienia certyfikatu należy wejść na stronę <http://certum.pl>, i z menu „Nasza oferta” wybrać „Certyfikaty SSL”. Później proszę wybrać odpowiedni typ certyfikatu i kliknąć przycisk „Kup” a następnie przejść do formularza zakupu i zarejestrować się.

Kup certyfikat Commercial SSL (niekwalifikowany)

— Żądanie certyfikatu

W poniższe pole wstaw żądanie certyfikatu (CSR).
żądanie certyfikatu można wygenerować:
- korzystając z generatora dostępnego na stronach CERTUM ([wygeneruj CSR](#))
- na serwerze na którym znajduje się zabezpieczona domena ([pobierz instrukcje dla swojej platformy](#))

```
-----BEGIN CERTIFICATE REQUEST-----
LQk+uTJQMz6P/gI/SRf9UxsZtkVtiA6mhWekkOPXfouL8GuEJFI+KQj9M/bCyeH
RDX+gUDrFMpSsHroJQ7UW0ZQn8W+FWK06iBceRL5VqazF8631HPaVGqIzHQIujFU
hIZB0dMq7SE5LnUypYJ71RXcGQV1S3VrifESNcFZiaEmIFoNPI8unU4+5nijPI8
ODGXchmFRkrvL57uwMxnSLDGFuQRyR89/T96fE0nXQBAMHPPfTJskpAvRUNAgMB
AAGgADANBgkqhkiG9w0BAQUFAAOCAQEABBYDA+aShTvrG7Jnnue7NNWzIEQe62+3
ERiPA7lIZiOuw/LBFM2cC7C9HFxpmIgzv9FwWed2C/4gCbrsYtgLlnlmJ0ixDhuP
a0Ck7yxvTgA9KnUTRY+H91ID8yriQ2BDD/KUPyQ79v+XnRQWpEjUWCnn/jkqRcSJ
GRKjv2iMORJUmGJNBLa7H8zSJM1N47iK536NNS0W5rXrrRU81gPbDJzPAbR4zgnV
ASBXTWcpPkzLbHxmpTFut8thffagWtqmHgTbbhAOC6lqitfE2jZi4AwEFd3tY7
6pYbM9wj1Cjmwv7PB/ozmGV5A07vKfHxbW93pVlc7ggQXV1yePIZg==
-----END CERTIFICATE REQUEST-----
```

— Adres email

Podaj adres e-mail, na który zostaną wysłane dalsze instrukcje postępowania.

E-mail:

— Dane do faktury

Nazwa:

NIP:

Ulica i nr:

Kod:

Miasto:

— Proszę wybrać formę płatności

Kwotę 242.78PLN (199PLN + 22% VAT) zapłać przelewem internetowym (eCard)

Kwota została uregulowana za pomocą karty zapłaty

Kwotę 242.78PLN (199PLN + 22% VAT) zapłać przelewem tradycyjnym

— Oświadczenie

ZANIM ZŁOŻYSZ WNIOSEK O WYDANIE CERTYFIKATU, POTWIERDZISZ GO, BĄDŹ UŻYJESZ DO REALIZACJI PIERWSZEGO PODPISU POWINIENES PRZECZYTAĆ TEKST NINIEJSZEGO OŚWIADCZENIA. JEŚLI NIE ZGADZASZ SIĘ Z WARUNKAMI NINIEJSZEGO OŚWIADCZENIA, NIE SKŁADAJ WNIOSKU O WYDANIE CERTYFIKATU, NIE POTWIERDZAJ I NIE UŻYWAJ GO.

Niniejsze oświadczenie obowiązuje od momentu przesłania przez Ciebie wniosku o wydanie certyfikatu do CERTUM - Powszechne Centrum Certyfikacji. Przedkładając wniosek o wydanie certyfikatu żądasz od organu je wydającego rozpatrzenia i wydania certyfikatu; jednocześnie oświadczasz, że akceptujesz warunki w nim określone.

Potwierdzam oświadczenie

W formularzu należy wkleić żądanie wygenerowane w poprzednim punkcie. Należy wkleić całą zawartość pliku żądania certyfikatu (łącznie z liniami -----BEGIN CERTIFICATE REQUEST----- i -----END CERTIFICATE REQUEST-----).

W następnej kolejności należy podać adres poczty e – mail, na który zostaną wysłane dalsze instrukcje postępowania i wybrać formę płatności. Proszę uważnie przeczytać oświadczenie, zaakceptować jego postanowienia i wybrać przycisk „Dalej”.

Na następnej stronie proszę przejrzeć dane i sprawdzić ich poprawność. Jeśli dane są poprawne należy wcisnąć przycisk „Dalej”, Pojawi się okno z danymi do przelewu i dokumentami wymaganymi do weryfikacji domeny.

Teraz należy czekać na maila aktywacyjnego. Będzie on podobny tego przedstawionego na rysunku:



Kolejnym krokiem będzie wejście na stronę podaną w wiadomości i wklejenie ID instalacyjnego certyfikatu.

3. Instalacja certyfikatu i klucza prywatnego

3.1. Eksport klucza prywatnego do formatu PKCS12

Kolejnym krokiem w procesie instalacji jest eksport certyfikatu serwera, certyfikatów urzędów pośrednich i głównego oraz klucza prywatnego do formatu PKCS12. Jest to zalecany format, jednak możliwe jest także korzystanie z magazynu certyfikatów platformy Java.

Zanim zostanie utworzony plik w formacie PKCS12 należy utworzyć plik z certyfikatami głównym pośrednim. Ze strony:

http://www.certum.pl/certum/cert,certyfikaty_zaswiadczenia_klucze.xml

należy pobrać główny certyfikat urzędu (Certum CA) oraz odpowiedni certyfikat urzędu pośredniego.

Należy zwrócić uwagę na nazwę urzędu, który wystawił certyfikat. Proszę pobrać certyfikaty w formacie dla serwerów WWW.

Następnie proszę otworzyć te dwa certyfikaty w edytorze tekstowym i skopiować ich zawartość do pliku bundle.crt. Plik bundle.crt powinien wyglądać podobnie do tego:

```

-----BEGIN CERTIFICATE-----
MIIDDDCCAfSgAwIBAgIDAQAqMA0GCSqGSIb3DQEBBQUAMD4xCzAJBgNVBAYTA1BM
MRswGQYDVQQKEExJVbml6ZXRvIFNwLiB6IG8uby4xEjAQBgNVBAMTCUN1cnR1bSBD
QTAEFw0wMjA2MTE5MDQ2MzlaFw0yNzA2MTE5MDQ2MzlaMD4xCzAJBgNVBAYTA1BM
MRswGQYDVQQKEExJVbml6ZXRvIFNwLiB6IG8uby4xEjAQBgNVBAMTCUN1cnR1bSBD
QTCCASIdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM6xwS7TT3zNjc4YPk/E
jG+AanPIW1H4m9LcuwBcsaD8dQPugfCI7iNS6eYVM42sLQnFdvkrOYCJ5JdLkKWo
ePhzQ3ukYbDYWMzhbGZ+nPMJX1VjhnWo7/OxLjBos8Q82KxujZlakE403Daa j4GI
ULdtlkIJ89eVgw1BS7Bqa/j8D35in2fE7SZfECYPCE/wpFcozo+47UX2bu4lXapu
Ob7kky/ZR6By6/qmW6/KUZ/iDsaWVhFu9+lmqSbYf5VT7QqFiLpPKaVCjF62/IUG
AKpoC6EahQGcxEZjgoi2IrHu/qpGWX7PNSzVttdp90gzFFS269lvzs2I1qsb2pY7
    
```

```
HVkCAwEAAaMTMBEwDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAAuI3O7+cUus/usESSbLQ5PqKEbq24IXfS1HeCh+YgQYHu4vgRt2PRFze+GXYkHAQaTOS9qmdvLdTN/mUxcMUbpqIKumB7bVjCmkn+YzILa+M6wKyrO7Do0w1RjBCDxjTgxSvGGrZgFCdsMneMvLJymM/NzD+5yCRCFNZX/OYmQ6kd5YCQzgNUKD73P9P4TelqCjqTE5s7FCMTY5w/0YcneeVMUeMBrYVdGjux1XMqPNPvG5k9VpWkKjHDkx0Dy5xO/fIR/RpbxXyEV6DHpx8Uq79AtoSqFlngNu8cN2bsWntgM6JQEhQDjXKKWYVIZQs6GAqm4VKQPNriiTsBhYscw==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIENTCCAax2gAwIBAgIDBHpSMA0GCSqGSIb3DQEgEBBQUAMD4xCzAJBgNVBAYTAlBMRswGQYDVQQKEExJVbml6ZXRvIFNwLiB6IG8uby4xejAQBgNVBAMTCUNlcnRlbSBDAQTAeFw0wOTAzMDMxMjUzMThaFw0yNDAzMDMxMjUzMThaMHcxZzAJBgNVBAYTAlBMSiWIAyDVQQKExlVbml6ZXRvIFRlY2hub2xvZ2llcyBTLkEuMScwJQYDVQQLEx5DZXJ0dW0gQ2VydG1maWNhdG1vbiBBdXR0b3JpdHkxGzAZBgNVBAMTEkNlcnRlbSBMZlB6IG8uby4xejAQBgNVBAMTCUNlcnRlbSBMZXZlbnCBJSBBDQTCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAAOCxNCMPiES6Xq/br1bWZFiLo8WLD1YFGQAXmWYELCk3SY2hlT+uAf6IhFeR3dwMUamme3UUbH+D4Pz0kv9ph0UEP0h91wAm6wx5rnA72ILVP1qGcqfXej11T2OI+yebf+drPhG2Q+bMERkCxo2fYsIPbF19yXSfU8vgd8/NKImo6StAcKgMa3F9w3pBDpJ4+y5ADiuorkCiPOURI+CFW/ZA+yiiFnSEhm3y+BM4f0z+dXtC/loUye5R2x20cxXz1P6It0MrebRHsazynvujfia3o3W+WGuzXt7Srow1OypWzvnZ6cxR+1R5ATyXECe0FK6az2q1bFYNySdT106lZ8CAwEAAaOCAQEwgf4wDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBByEFIBiEd7Aa6cQ4QjwVbQwg7/6jwhgMFIGAlUdIwRLMEMhQqRAMD4xCzAJBgNVBAYTAlBMMRswGQYDVQQKEExJVbml6ZXRvIFNwLiB6IG8uby4xejAQBgNVBAMTCUNlcnRlbSBBDQYIDAQAUMCwGA1UdHwQ1MCMwIaAfOB2GG2h0dHA6Ly9jcmwU2VydHVtLnBsL2NhLmNyYbDA6BgNVHSAEMzAxCzAJBgNVBAYTAlBMBggrBgEFBQcCARYZaHR0cHM6Ly93d3cuY2VydHVtLnBsL0NQzANBgkqhkiG9w0BAQUFAAOCAQEAsNjXnyR8Fw+yTKdUAQlhhK+kioXhh06Nxn7mrFWDHBZwFjDvplupCXpLp+4a5J8nXK5ULMLiipBq+gCOTw/JBG9HOEhdCO802JxGDTL67lHAXECAVkgVlJ2++3p96m/iomkc3ZZDqVYG7BWT1YzshoWjNxmDwI0bRiChqNwwdju/RHjP822wQWhr1N4jFg8UcjujSpinAT9kTn7aVAdeqhuhdztaW4yTYppRNsxySwShk/c0NC2p0sit0H1k+muyUirojTGXFsc2FUcr8MQtFuV2Peip7Qs++4aOB6acu5ROf4bnKWpWz5sMktU2b849oYkS3RbEhar/71/cMkYbrA==
-----END CERTIFICATE-----
```

Następnie proszę wydać następującą komendę:

```
pkcs12 -export -in 295925.cer -inkey tomcat.key -out tomcat.pfx -certfile bundle.crt
```

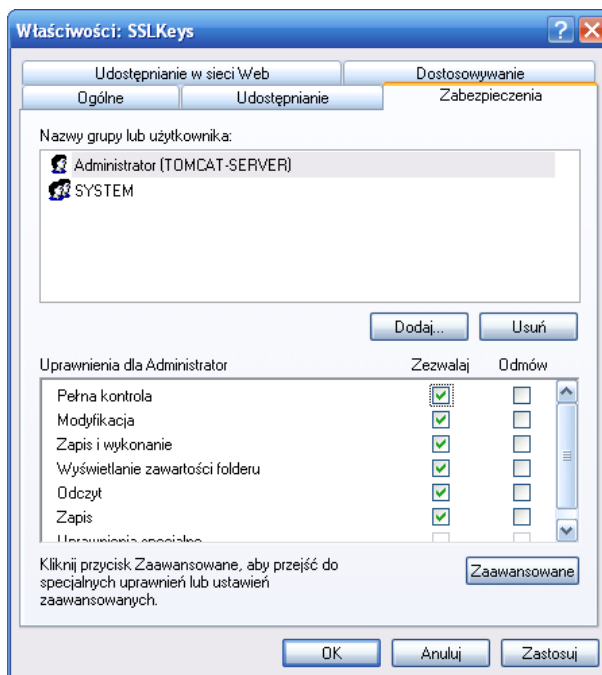
295925.cer to plik certyfikatu pobranego z repozitorium certyfikatów Certum, tomcat.key to klucz prywatny wygenerowany w kroku pierwszym a bundle.crt to plik z certyfikatami urzędów CERTUM tomcat.pfx to plik w formacie PKCS12. Należy podać hasło zabezpieczające klucz w pliku tomcat.key oraz podać nowe hasło chroniące klucz w formacie PKCS12.

3.2. Zmiana konfiguracji serwera Tomcat

Aby włączyć SSL należy skopiować plik `tomcat.pfx` w bezpieczne miejsce na dysku twardym serwera. Należy nadać odpowiednie uprawnienia do katalogu z plikiem `tomcat.pfx`.

Na potrzeby tego dokumentu plik `tomcat.pfx` zapisano w katalogu `C:\Program Files\Apache Software Foundation\Tomcat 6.0\SSLKeys`.

Uprawnienia do tego katalogu powinny wyglądać następująco:



Tylko Administrator i konto SYSTEM powinny mieć pełen dostęp do tego katalogu. Takie same uprawnienia należy nadać plikowi `C:\Program Files\Apache Software Foundation\Tomcat 6.0\conf\server.xml`.

Następnie należy edytować plik `server.xml`. W pliku tym trzeba odnaleźć sekcję zaczynającą się od fragmentu:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443
```

Teraz powinno się usunąć komentarze przed i za tagiem `<connector>` (odpowiednio `<!--` i `-->`). Należy zmienić parametry połączenia SSL. Właściwość `port` powinna wynosić `443`, `sslProtocol` TLS. Należy dodać trzy właściwości – `keystoreFile`, `keystorePass` oraz `keystoreType`. Pierwszej z nich należy nadać wartość:

```
„C:\Program Files\Apache Software Foundation\Tomcat 6.0\SSLKeys\tomcat.pfx”
```

drugiej natomiast hasło jakie przypisane zostało przy eksporcie klucza prywatnego do formatu PKCS12. Trzeciej należy nadać wartość PKCS12.

Cała sekcja powinna wyglądać następująco:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443
This connector uses the JSSE configuration, when using APR, the
connector should be using the OpenSSL style configuration
described in the APR documentation -->

<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="C:\Program Files\Apache Software Foundation\Tomcat 6.0\SSLKeys\tomcat.pfx"
keystorePass="
keystoreType="PKCS12"
/>
```

Ostatnim krokiem jest ponowne uruchomienie serwera Tomcat. W wierszu polecenia trzeba wydać polecenia "net stop Apache Tomcat" i net start "Apache Tomcat".

```
C:\Documents and Settings\Administrator>net stop "Apache Tomcat"
Usługa Apache Tomcat jest właśnie zatrzymywana.
Usługa Apache Tomcat została zatrzymana pomyślnie.
```

```
C:\Documents and Settings\Administrator>net start "Apache Tomcat"
```

```
Usługa Apache Tomcat jest właśnie uruchamiana.
Pomyślnie uruchomiono usługę Apache Tomcat.
```

4. Uwierzytelnianie użytkowników na podstawie certyfikatów klucza publicznego

Protokoły SSL w wersji 3 i TLS umożliwiają dwustronne uwierzytelnianie. Zwykle wykorzystuje się tylko uwierzytelnianie serwera, jednak możliwe jest także uwierzytelnianie użytkowników i kontrola dostępu do serwera WWW poprzez użycie certyfikatów użytkowników.

4.1. Instalacja certyfikatów Urzędu Certyfikacji Certum CA

Ze strony Certum należy pobrać certyfikat głównego urzędu certyfikacji Certum CA oraz podrzędnego urzędu certyfikacji.

W tym celu powinno się przejść do strony certum.pl i z górnego menu wybrać pozycję „Obsługa certyfikatów”, a następnie „Klucze i zaświadczenia”.

Jeśli certyfikaty użytkowników zostały wystawione przez urząd Certum Level II należy pobrać certyfikaty urzędu Certum CA i Certum Level II. Analogicznie postępuje się z innymi poziomami (Level I, III i IV). Jako typ certyfikatu trzeba wybrać „Certyfikat dla Przeglądarek Internetowych” i zapisać je w katalogu C:\Program Files\Apache Software Foundation\Tomcat 6.0\SSLKeys jako pliki Certum CA.cer i Certum Level II.cer.

Kolejnym krokiem jest import certyfikatów urzędów certyfikacji do magazynu certyfikatów Javy. W tym celu należy otworzyć wiersz polecenia i przejść do katalogu %Java%\jre\bin, gdzie zmienna %Java% to nazwa katalogu z najnowszą wersją maszyny wirtualnej Java. W przedstawionym przypadku jest to katalog C:\Program Files\Java\jre6\bin.

Teraz trzeba wydać polecenie:

```
keytool.exe -import -keystore "C:\Program  
Files\Java\jre6\lib\security\cacerts" -file "C:\Program Files\Apache  
Software Foundation\Tomcat 6.0\SSLKeys\Certum CA.cer" -alias CertumCA
```

a następnie:

```
keytool.exe -import -keystore "C:\Program  
Files\Java\jre6\lib\security\cacerts" -file "C:\Program \ Files\Apache  
Software Foundation\Tomcat 6.0\SSLKeys\Certum Level II.cer" -alias  
CertumLevelII
```

Domyślnym hasłem dla magazynu certyfikatów Javy jest „changeit”. Wskazane jest zmienienie tego hasła.

4.2. Edycja plików konfiguracyjnych

Kolejnym krokiem jest zmiana konfiguracji serwera Tomcat. Należy wprowadzić zmiany w trzech plikach konfiguracyjnych: web.xml, server.xml i tomcat-users.xml. Znajdują się one w katalogu C:\Program Files\Apache Software Foundation\Tomcat 6.0\conf.

4.3. Plik server.xml

Należy odnaleźć sekcję konfiguracji połączenia SSL. Jest to tag <Connector> - ten sam, który został zmieniony w poprzedniej części tego przewodnika. Należy zmienić wartość clientAuth z false na true.

4.4. Plik tomcat-users.xml

W tym definiuje się role a także użytkowników, którzy mają mieć dostęp do witryny obsługiwanej przez serwer Tomcat. Znajduje się tam przynajmniej jeden wpis definiujący użytkownika:

```
<user username="admin" password="f9E28cck7" roles="admin,manager"/>
```

Po tym wpisie należy dodać kolejną linijkę, np.:

```
<user name="Jaroslaw Mila" password="null"/>
```

Szczególną uwagę należy zwrócić na właściwość user name – musi być ona identyczna jak pole Common Name certyfikatu użytkownika.

4.5. Plik web.xml

Tuż po tagu <web-app> należy dodać następujące wpisy:

```
<login-config>  
    <auth-method>CLIENT-CERT</auth-method>  
    <realm-name>Client Cert Users-only Area</realm-name>  
</login-config>
```

Konfiguracja serwera została zakończona. Teraz wystarczy uruchomić go ponownie.

Ostatnim krokiem jest zainstalowanie certyfikatów i kluczy prywatnych w magazynie certyfikatów przeglądarki internetowej klienta. Poradniki opisujące jak zainstalować certyfikaty i klucze prywatne użytkownika znajdują się na stronie:

http://www.certum.pl/certum/cert,wiedza_instrukcje.xml.