

Konwertuj certyfikat

Article Number: 582 | Rating: Unrated | Last Updated: Wed, May 22, 2019 10:14 AM

Format PEM

Jest to format obsługiwany przez serwer Apache i inne serwery tego typu. Cechą charakterystyczną w tym formacie jest obecność sekcji -----BEGIN----- i -----END----- . Certyfikat serwera, certyfikat pośredni i klucz prywatny mogą być zapisane w formacie PEM odpowiednio z rozszerzeniem .crt, .cer i .key lub .pem.

Format DER

Format DER jest binarną formą certyfikatu i jest formatem typowym dla platform Java. Może mieć zarówno rozszerzenie .der jak i .cer jednak w odróżnieniu od formatu PEM (który także może mieć takie rozszerzenia) nie zawiera sekcji BEGIN i END a jedynie zaszyfrowaną treść.

Format PKCS#7 / P7B

Format obsługiwany przez platformy Microsoft Windows i Java Tomcat. Najczęstszym rozszerzeniem jest .p7b lub .p7c. Plik P7B zawiera jedynie certyfikat wraz z certyfikatami Urzędu Certyfikacji (chain certificates) bez klucza prywatnego. Certyfikaty P7B zawierają sekcje -----BEGIN PKCS7----- i -----END PKCS7-----.

Format PKCS#12 / PFX

Pliki te są wykorzystywane na serwerach Windows do eksportu i importu certyfikatu i klucza prywatnego. Format PFX jest formatem binarnym, który gromadzi certyfikat serwera, certyfikaty pośrednie i klucz prywatny w jednym pliku. Typowe rozszerzenia to .pfx lub .p12.

Alternatywna metoda konwersji formatu PEM

Ze względów bezpieczeństwa rekomendowanym sposobem konwertowania certyfikatu jest przeprowadzenie tej operacji bezpośrednio na serwerze, służą temu poniższe komendy:

- **Konwertuj PEM na DER (dla certyfikatu)**

Linux command line

```
openssl x509 -outform der -in cert.pem -out cert.der
```

- **Konwertuj PEM na DER (dla klucza prywatnego)**

Linux command line

```
openssl rsa -in key.pem -outform DER -out key.der
```

- **Konwertuj PEM na P7B**

Linux command line

```
openssl crl2pkcs7 -nocrl -certfile cert.pem -out cert.p7b -certfile rootca.pem
```

- **Konwertuj PEM na PFX**

Linux command line

```
openssl pkcs12 -export -out cert.pfx -inkey key.pem -in cert.pem -certfile rootca.pem
```

Alternatywna metoda konwersji formatu **DER**

- **Konwertuj DER na PEM (dla certyfikatu)**

Linux command line

```
openssl x509 -inform der -in cert.der -out cert.pem
```

- **Konwertuj DER na PEM (dla klucza prywatnego)**

Linux command line

```
openssl rsa -in key.der -inform DER -out key.pem
```

Alternatywna metoda konwersji formatu **P7B**

- **Konwertuj P7B na PEM**

Linux command line

```
openssl pkcs7 -print_certs -in cert.p7b -out cert.pem
```

- **Konwertuj P7B na PFX**

Linux command line

```
openssl pkcs7 -print_certs -in cert.p7b -out cert.pem
```

Linux command line

```
openssl pkcs12 -export -out cert.pfx -inkey key.pem -in cert.pem -certfile rootca.pem
```

Alternatywna metoda konwersji formatu **PFX**

- **Konwertuj PFX na PEM**

Linux command line

```
openssl pkcs12 -in cert.pfx -out cert.pem -nodes
```

Ze względów bezpieczeństwa połączenie ze stroną jest chronione certyfikatem SSL. Podane przez Ciebie informacje nie są przez nas przechowywane i są dostępne jedynie podczas bieżącej sesji przeglądarki.

Posted - Wed, May 22, 2019 10:14 AM. This article has been viewed 1029 times.

Online URL: <http://kb.ictbanking.net/article.php?id=582>