Certificados PEM

Cómo crear un archivo .pem para instalaciones de certificados SSL

¿Que es un certificado pem?

Los archivos Privacy Enhanced Mail (PEM) son contenedores de certificados concatenados que se usan con frecuencia en instalaciones de certificados cuando se importan múltiples certificados que forman una cadena completa como un solo archivo. Son un estándar definido en los RFC 1421 a 1424

Se los puede considerar como un contenedor en capas de certificados encadenados. Un archivo .pem es un formato contenedor que puede incluir el certificado público o toda la cadena de certificados (clave privada, clave pública, certificados raíz):

Llave privada (.key)
Certificado de servidor (crt, clave pública)
(opcional) CA intermedia y / o paquetes si están firmados por un tercero

¿Cómo crear un archivo PEM autofirmado?

```
openssl req -newkey rsa: 2048 -new -nodes -x509 -days 3650 -keyout key. pem -out cert. pem
```

¿Cómo crear un archivo PEM a partir de archivos de certificados

existentes que forman una cadena?

(opcional) Elimina la contraseña de la clave privada siguiendo los pasos que se detallan a continuación:

```
openssl rsa -in server.key -out nopassword.key
```

Nota: Tienes que introducir la contraseña de la clave privada.Combine la clave privada, el certificado público y cualquier archivo de certificado intermedio de terceros:

```
cat nopassword.key > server.pem<br />cat server.crt >> server.pem
```

Nota: Repite este paso según sea necesario para archivos de cadena de certificados de terceros, paquetes, etc.

```
cat intermediate.crt >> server.pem
```

También se puede realizar desde un editor:

Abre un editor de texto (como wordpad) y pega todo el cuerpo de cada certificado en un archivo de texto en el siguiente orden:

La clave privada: your_domain_name.key
El Certificado Primario - your_domain_name.crt
El Certificado Intermedio - DigiCertCA.crt
El certificado raíz - TrustedRoot.crt

----BEGIN RSA PRIVATE KEY-----
(Your Private Key: your_domain_name.key)
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: your_domain_name.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: DigiCertCA.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----

Crear un PFX a partir del certificado PEM

Parámetro	Descripción
openssl	The command for executing OpenSSL.
pkcs12	The file utility for PKCS#12 files in OpenSSL.
-export -out certificate.pfx	Exports and saves the PFX file as certificate.pfx.
-inkey privateKey.key	Uses the private key file privateKey.key as the private key to combine with the certificate.
-in certificate.crt	Uses certificate.crt as the certificate to combine with the private key.

```
openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in certificate.crt -certfile
```

Otro método

1. Take the file you exported (e.g. certname.pfx) and copy it to a system where you have OpenSSL installed. Note: the *.pfx file is in PKCS#12 format and includes both the certificate and the private key.
2. Run the following command to export the private key: `openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes`
3. Run the following command to export the certificate: `openssl pkcs12 -in certname.pfx -nokeys -out cert.pem`
4. Run the following command to remove the passphrase from the private key: `openssl rsa -in key.pem -out server.key`

Revision #3
Created 17 May 2022 17:56:55 by Admin
Updated 17 May 2022 17:58:48 by Admin