How to create a .pem file for SSL Certificate Installations

suse.com/support/kb/doc

SUSE Support

Here When You Need Us

This document **(7013103)** is provided subject to the disclaimer at the end of this document.

Environment

SUSE Linux Enterprise Server

Situation

How to create a .pem file for SSL Certificate Installations

Resolution

Privacy Enhanced Mail (PEM) files are concatenated certificate containers frequently used in certificate installations when multiple certificates that form a complete chain are being imported as a single file. They are a defined standard in RFCs 1421 through 1424. They can be thought of as a layered container of chained certificates. A *.pem* file is a container format that may just include the public certificate or the entire certificate chain (private key, public key, root certificates):

- Private Key
- Server Certificate (crt, puplic key)
- *(optional) Intermediate CA and/or bundles if signed by a 3rd party*

How to create a self-signed PEM file

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

How to create a PEM file from existing certificate files that form a chain

- *(optional)* Remove the password from the Private Key by following the steps listed below:

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

  Note: Enter the pass phrase of the Private Key.

- Combine the private key, public certificate and any 3rd party intermediate certificate files:

  ```
  cat nopassword.key > server.pem
  cat server.crt >> server.pem
  ```

  Note: Repeat this step as needed for third-party certificate chain files, bundles, etc:

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

Cause

Additional Information

How to create a PEM file with the help of an automated script:

- Download NetIQ Cool Tool OpenSSL-Toolkit.
- Select Create Certificates | PEM with key and entire trust chain
- Provide the full path to the directory containing the certificate files.
- Provide the filenames of the following:
  - private key
  - public key (server crt)
  - *(conditional) password for private key*
  - *(conditional) any intermediate certificate chain file(s)*

For additional information, please see TID 7015502 - Common Mistakes in SSL Certificate Management & Implementation.

The following details the structure of a typical .pem file (including the entire certificate chain):

```
-----BEGIN RSA PRIVATE KEY-----
(Private Key: domain_name.key contents)
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Primary SSL certificate: domain_name.crt contents)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Intermediate certificate: certChainCA.crt contents)
-----END CERTIFICATE----
```

Disclaimer

This Support Knowledgebase provides a valuable tool for SUSE customers and parties interested in our products and solutions to acquire information, ideas and learn from one another. Materials are provided for informational, personal or non-commercial use within your organization and are presented "AS IS" WITHOUT WARRANTY OF ANY KIND.

- **Document ID:***7013103*
- **Creation Date:** 26-Aug-2013
- **Modified Date:**03-Mar-2020
- SUSE Linux Enterprise Server

< Back to Support Search

For questions or concerns with the SUSE Knowledgebase please contact: tidfeedback@suse.com

SUSE Support Forums

Get your questions answered by experienced Sys Ops or interact with other SUSE community experts.

Join Our Community

Open an Incident

Open an incident with SUSE Technical Support, manage your subscriptions, download patches, or manage user access.

Go to Customer Center