Generating a CSR for an S/MIME Personal certificate using OpenSSL

Openprovider’s SSL panel currently does not support generating a CSR for S/MIME Personal Certificates, which requires an email address in the ‘Common Name’ field. OpenSSL is a versatile command-line tool widely used across UNIX, Linux, BSD, and Windows systems for managing cryptographic operations. This guide outlines the steps to create a private key and CSR, essential for obtaining an email signing certificate (also known as an S/MIME or client certificate).

Prerequisites

- Ensure OpenSSL is installed on your system.
- Create a secure directory to store your private key and CSR files.
- Protect this directory to prevent unauthorized access.

Step-by-Step Instructions

1. **Open the Terminal**
   Launch the terminal application on your computer.

2. **Generate the Private Key and CSR**
   Execute the following command:

   ```
   openssl req -nodes -newkey rsa:2048 -keyout certificate.key -out certificate.csr
   ```

   This command creates a 2048-bit RSA private key (certificate.key) and a CSR (certificate.csr).

3. **Provide Certificate Details**
   You'll be prompted to enter the following information:
4. - ◦ **Country Name** (2-letter code): e.g., NL
     ◦ **State or Province Name**: e.g., Gelderland
     ◦ **Locality Name**: e.g., Nijmegen
     ◦ **Organization Name**: e.g., Your Company Name
     ◦ **Organizational Unit Name**: e.g., IT Department

- **Common Name**: Your Email address for which the S/MIME Personal certificate to be generated
- **Email Address**: Contact point of the certificate owner e.g., john.doe@example.com
- **Challenge Password (Optional)**: (Leave blank)
- **Optional Company Name**: (Leave blank)

- **Review and Save the CSR**
  The certificate.csr file is now created in your current directory. Open this file with a text editor and copy its entire contents, including the -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST----- lines.

- **Submit the CSR**
  Paste the copied CSR into the appropriate field during the certificate ordering process on your Openprovider SSL panel.

  After purchasing the certificate please refer https://openprovider.help/books/ssl-certificates/page/how-to-generate-public-key-pfx to generate a PFX certificate using OpenSSL to use with email client like outlook.

  Note: Always keep your private key (certificate.key) secure and never share it.

Revision #3
Created 2026-08-07 14:31:23 UTC by Sarath
Updated 2026-08-19 14:36:44 UTC by Sarath