Certificate Signing Request

Summary

A CSR, short for Certificate Signing Request, is required for accessing ADP APIs and authenticating users with SSO. This document describes the steps for generating a CSR using OpenSSL. Other tools (e.g. Java Keytool) can be used to generate a CSR are not covered in this document.

Target Audience

This document is to be used by ADP clients. If you are a Marketplace partner developer, your partner onboarding team will guide you through the process.

Step by Step Guide

1. Download OpenSSL Light for Windows at:http://slproweb.com/products/Win32OpenSSL.html. Mac Users can open Terminal and jump to the OpenSSL commands in Step 7 below
2. Follow the instructions in the install wizard to install OpenSSL.
3. Go to the location where you installed OpenSSL (e.g. **C:\OpenSSL-Win32\bin**) and modify the file: "**C:\OpenSSL-Win32\bin\openssl.cfg**". Look for the section starting with "req_attributes", remove "unstructuredName", and save the file
    - Original:

      [req_attributes]

      challengePassword = A challenge password

      challengePassword_min = 4

      challengePassword_max = 20

      unstructuredName = An optional company name

      Modified:
      [req_attributes]
      challengePassword = A challenge password
      challengePassword_min = 4
      challengePassword_max = 20
4. Open cmd.exe
5. Go to the location where you installed OpenSSL
    - cd **C:\OpenSSL-Win32\bin**
6. If you are using a Windows machine, set the following variable.
    - set OPENSSL_CONF=**C:\OpenSSL-Win32\bin\openssl.cfg**
7. Generate the CSR:
    - openssl genrsa -out *companyname_auth*.key 2048
    - openssl req -new -key *companyname_auth*.key -out *companyname_auth*.csr
    - **Note: Your CSR must not request S/MIME capabilities.**
8. Enter the following information into your certificate signing request. Please leave the challenge password blank.
    - Country Name
    - State or Province Name
    - Locality Name
    - Organization Name
    - Common Name – Use something meaningful (g. CompanyName Corp Mutual SSL) or whatever best describes the usage and identifies this as the Mutual SSL Authentication certificate.
    - A challenge password – Leave this field blank.
9. Email the *companyname_auth*.csr file as an attachment to your ADP representative.
10. Save the signed certificate from ADP into a file named *companyname_auth*.pem in the same location that you created the CSR originally (C:\OpenSSL-Win32\bin).
11. If you are using Windows/IIS, use the commands below to get the key and certificate in PKCS12 format.
    - openssl pkcs12 -export -out *companyname_auth*.pfx -name "*Company Name Mutual SSL*" -inkey *companyname_auth*.key -in *companyname_auth*.pem
12. Enter Export Password.

The resulting certificate and key should be in the file ***companyname_auth*.pfx** that you will reference for Mutual SSL authentication.

Important: Make sure you safeguard the .key, .pfx and .jks files. Anyone that possesses these confidential files has access to the web service.