

# Certificate Signing Request

## FOR ADP AUTHORIZED USERS ONLY

All Rights Reserved. These materials may not be reproduced in any format without the express written permission of ADP, LLC.

ADP provides this publication “as is” without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. ADP is not responsible for any technical inaccuracies or typographical errors which may be contained in this publication. Changes are periodically made to the information herein, and such changes will be incorporated in new editions of this publication. ADP may make improvements and/or changes in the product and/or the programs described in this publication.

## CONTENTS

- [Overview](#)
- [Audience](#)
- [Completing a Certificate Signing Request](#)

## Overview

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

## Audience

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

## Completing a Certificate Signing Request

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.
2. Follow the instructions in the Install Wizard to install OpenSSL.
3. Go to the location where you installed OpenSSL (for example, **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 click **Save**.

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 and at the command line, type `cd C:\OpenSSL-Win32\bin`.
6. If you are using a Windows machine, set the following variable: `set OPENSSSL_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. Leave the challenge password blank.
  - Country Name
  - State or Province Name
  - Locality Name
  - Organization Name
  - Common Name (Use something meaningful, such as *CompanyName Corp Mutual SSL* or whatever best describes the usage and identifies this as the Mutual SSL Authentication certificate)
  - 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 initially created the CSR (**C:\OpenSSL-Win32\bin**).
11. If you are using Windows/IIS, use the following command 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.