Chapter 2

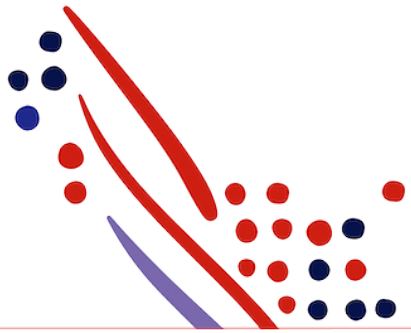
Certificate Signing Request

from ADP Marketplace ESI - Getting started

Published on
Mar 22, 2022, 09:18 AM

Last modified
Jul 15, 2025, 02:47 PM

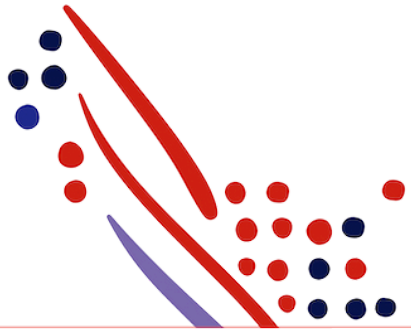
Always Designing for People™



ADP Copyright Information

Published on
Mar 22, 2022, 09:18 AM

Published on
Jul 15, 2025, 02:47 PM



Chapter Contents

Chapter 2

Certificate Signing Request

A private key and matching Web Services (WS) Certificate are required to access the ADP Marketplace web services. The WS Certificate provides client information to ADP and the matching private key confirms the authenticity of the client. To generate the WS Certificate a Certificate Signing Request (CSR) needs to be generated by the client. During the CSR generation the private key and matching public key are created. The CSR is submitted to the ADP Web Services Certificate Authority *(currently run by Sectigo)* and they return the WS Certificate.

Many software tools store the private key and the WS Certificate in one Personal Information Exchange Format (PFX) file, also known as P12- file.

Disclosure

Open Secure Sockets Layer (OpenSSL) is an open source tool. Although ADP has tested the commands, based on the OS and version configuration settings and other environmental factors as well as the commands and configuration may have to be adjusted. ADP does not support OpenSSL tool itself. For questions and support please reach out to your IT department and/or third party.

Other tools (such as Java Keytool), that can be used to generate a CSR, are not covered in this document. If another tool is used, please make sure the CSR is PEM format (base64 encoded with additional header and footer lines).

Clients need to ensure that every time new private and public keys are created, they are managed properly. If they are generated more than once, each key pair must be stored (possibly in different directories) so there is no confusion. In addition, the returned Web Services Certificate (which also contains the public key) must be managed properly (stored in the directory that has the matching private key).

Install OpenSSL Light for Windows

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 3.
2. Follow the instructions in the Install Wizard. All options can be left default.

CSR for a new connection

1. Open **cmd.exe.**
2. Go to the location where you installed OpenSSL and set the current directory to the **bin** directory, for example **cd C:\Program Files\OpenSSL-Win64\bin**.
3. Using the commands below to generate the CSR and private key to a folder of choice, for example **C:\Temp**. Replace companyname_auth by the value you want to use.

    - openssl genrsa -out C:\Temp\companyname_auth.key 2048
    - openssl req -new -key C:\Temp\companyname_auth.key -out C:\Temp\companyname_auth.csr

    > **Note**
    >
    > Your CSR must not request S/MIME capabilities.

4. Enter the information below into your CSR. Other fields can be left empty.

    - Country Name
    - State or Province Name
    - Locality Name
    - Organization Name
    - Common Name
    - Leave Challenge password blank *(i.e. no password)*

    > **Note**
    >
    > - Please contact your ADP Representative for the values to be used for **Organization Name** and **Common Name**.
    > - For Country Name use the ISO compliant 2 letter code, for example NL.

- If you enter an e-mail address, please make sure it is an existing group e-mail address we can use to send notifications to on certificate expiration.

5. Attach the CSR to the ADP eService ticket. Please also a provide a **group e-mail address** to be automatically notified when the generated certificate is approaching its two-year expiration date.

> **Important**
>
> - Please make sure to store the generated private key in a safe location. It is needed to setup a connection to ADP Marketplace. Never give the private key to unauthorized parties and never send it via unsecure connections.
> - The private key should **not** be send to ADP.
> - Please make sure the values used for **Organization Name** and **Common Name** are stored. You will need them when the current certificate is going to expire to generate a new CSR.

6. After receiving the e-mail from ADP with download links for your certificate. Please download and save the signed certificate. The downloaded certificate together with the private key are needed to connect to the ADP web services.

> **Tip**
>
> If you are using Windows/IIS you can use the following command to combine the private key and certificate in PKCS12 format file (.pfx):
>
> openssl pkcs12 -export -out *companyname_auth*.pfx -name "*Company Name Mutual SSL*" -inkey *companyname_auth*.key -in *companyname_auth*.pem.
>
> If needed replace *companyname_auth* with the correct name. The resulting .pfx file can be used for mutual SSL authentication.

CSR for certificate renewal

1. Create the CSR, see *Certificate Signing Request for a new connection*.

> **Important**
>
> Make sure the values for **Organization Name** and **Common Name** match the values used for the initial CSR and current certificate ***exactly***. When in doubt contact your ADP Representative to check the values. Using the wrong values will result in loss of connection.

2. After you have created your CSR, you have two options for submitting it to ADP for signing:

    1. Mail the CSR to marketplace esi client support@adp.com for processing or,
    2. Submit your request directly to ADP security Services:

        - Open the ADP Certificate Signing Tool.
        - Enter your e-mail address and click [Submit].
        - Click [Enroll Certificate].
        - For Certificate Profile choose **Authentication and Transaction Signing**.
        - Upload the CSR via the button [Upload CSR] or paste the complete contents including the BEGIN CERTIFICATE REQUEST and END CERTIFICATE REQUEST lines of your CSR into the CSR text box.
        - Enter the following information in the Custom Fields:
            - Company name

> **Note**
>
> This value has to be an exact match of the value of the Organization you chose when creating the CSR.

- Your ADP Client ID

> **Note**
>
> Please contact your ADP Representative for your ADP Client ID.

- Your technical contact's first and last name.
- Your technical contact's e-mail address. The certificate will be sent to this address.

> **Tip**
>
> Please use group distribution list or group e-mail address as this address will also be used to automatically notify you when the generated certificate is approaching its two-year expiration date.

- Click 'Submit'.

> **Note**
>
> It might take up to a week for you to receive the certificate.

> **Important**
>
> Make sure you safeguard the .key, .pfx and .jks files. Anyone that possesses these confidential files can potentially access to the web service.