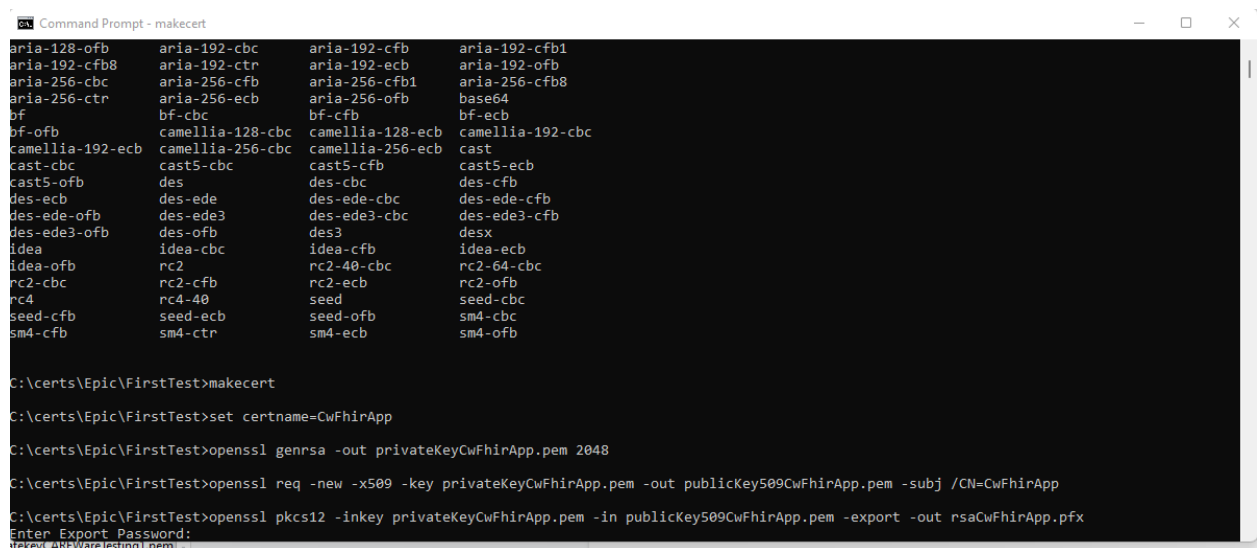


Generating RSA keys for the CAREWare PDI FHIR Datasource

Follow these instructions to generate RSA keys to connect a CAREWare PDI FHIR Datasource with an EMR FHIR App.

1. Install OpenSSL from these binaries: OpenSSL for Windows Pre-compiled Win32/64 at <https://wiki.openssl.org/index.php/Binaries> .
2. Make a directory where you want your .PEM and .PFX files to be created. Copy makecert.bat to that directory.
3. Open a command window and navigate to the directory where you put makecert.bat.
4. To check if the openssl bin folder is in your environment variable PATH list, do the following.
 - At the command prompt enter: **openssl** .
 - If you get a list of available openssl commands, you're good; otherwise check your openssl installation.
5. At the command prompt enter: **makecert** . Your command window should prompt you for your pfx password, which you will later need to set up your CAREWare PDI FHIR Data Source.



```
Command Prompt - makecert
aria-128-ofb      aria-192-cbc      aria-192-cfb      aria-192-cfb1
aria-192-cfb8    aria-192-ctr      aria-192-ecb      aria-192-ofb
aria-256-cbc     aria-256-cfb      aria-256-cfb1     aria-256-cfb8
aria-256-ctr     bf-cbc           bf-cfb           base64
bf-ofb          camellia-128-cbc  camellia-128-ecb  camellia-192-cbc
camellia-192-ecb camellia-256-cbc  camellia-256-ecb  cast
cast-cbc        cast5-cbc        cast5-cfb        cast5-ecb
cast5-ofb       des              des-cbc          des-cfb
des-ecb         des-ede         des-ede-cbc      des-ede-cfb
des-ede-ofb     des-ede3        des-ede3-cbc     des-ede3-cfb
des-ede3-ofb    des-ofb         des3             desx
idea            idea-cbc         idea-cfb         idea-ecb
idea-ofb        rc2              rc2-40-cbc       rc2-64-cbc
rc2-cbc         rc2-cfb         rc2-ecb          rc2-ofb
rc4             rc4-40          seed             seed-cbc
seed-cfb       seed-ecb        sm4-cbc          sm4-cfb
sm4-cfb        sm4-ctr         sm4-ecb          sm4-ofb

C:\certs\Epic\FirstTest>makecert

C:\certs\Epic\FirstTest>set certname=CwFhirApp

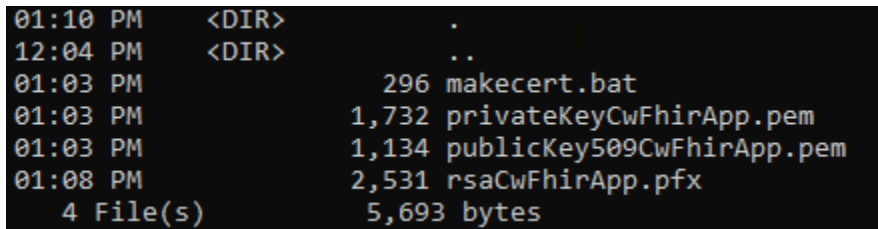
C:\certs\Epic\FirstTest>openssl genrsa -out privateKeyCwFhirApp.pem 2048

C:\certs\Epic\FirstTest>openssl req -new -x509 -key privateKeyCwFhirApp.pem -out publicKey509CwFhirApp.pem -subj /CN=CwFhirApp

C:\certs\Epic\FirstTest>openssl pkcs12 -inkey privateKeyCwFhirApp.pem -in publicKey509CwFhirApp.pem -export -out rsaCwFhirApp.pfx
Enter Export Password:
C:\certs\Epic\FirstTest>CAREWareTesting1.pem
```

6. At the command prompt, enter the password and then confirm the password.

7. At the command prompt enter: **dir** . You should see the following files:



```
01:10 PM    <DIR>      .
12:04 PM    <DIR>      ..
01:03 PM                296 makecert.bat
01:03 PM            1,732 privateKeyCwFhirApp.pem
01:03 PM            1,134 publicKey509CwFhirApp.pem
01:08 PM            2,531 rsaCwFhirApp.pfx
         4 File(s)      5,693 bytes
```

The file rsaCwFhirApp.pfx is a password-protected file which contains the randomly generated public key and the private key that match the data in the two .PEM files. This .PFX file, along with the password, is required to set up a PDI FHIR Datasource on the CAREWare side.

The file publicKey509CwFhirApp.pem is what you use at your EMR's FHIR App setup screen when it asks for the public key. During this setup of the FHIR App on the EMR side, you should save some key information that CAREWare will need: The Client ID, the Non-production Client ID, and any URL information (if it is provided at this time). The Client ID is a unique EMR-assigned key that identifies the CAREWare PDI FHIR Datasource you plan to use at the EMR's authentication server.

privateKeyCwFhirApp.pem was only created as a step in the process to make the pfx file. It should be safely stored with the other keys or deleted. If a bad actor gets your private key, he or she can use FHIR to get medical information from your EMR under your name. You can always get your private key again using OpenSSL and your .PFX file as long as you have your password.

These three .PEM and .PFX files only work with each other. If you need another PDI FHIR Datasource to connect to another EMR instance, you should use makecert.bat and make a fresh set of keys to use for that connection.

If you do not have makecert.bat, then you can make your own batch file with the following text:

```
set certname=CwFhirApp

openssl genrsa -out privateKey%certname%.pem 2048

openssl req -new -x509 -key privateKey%certname%.pem -out publicKey509%certname%.pem -subj /CN=%certname%

openssl pkcs12 -inkey privateKey%certname%.pem -in publicKey509%certname%.pem -export -out rsa%certname%.pfx
```