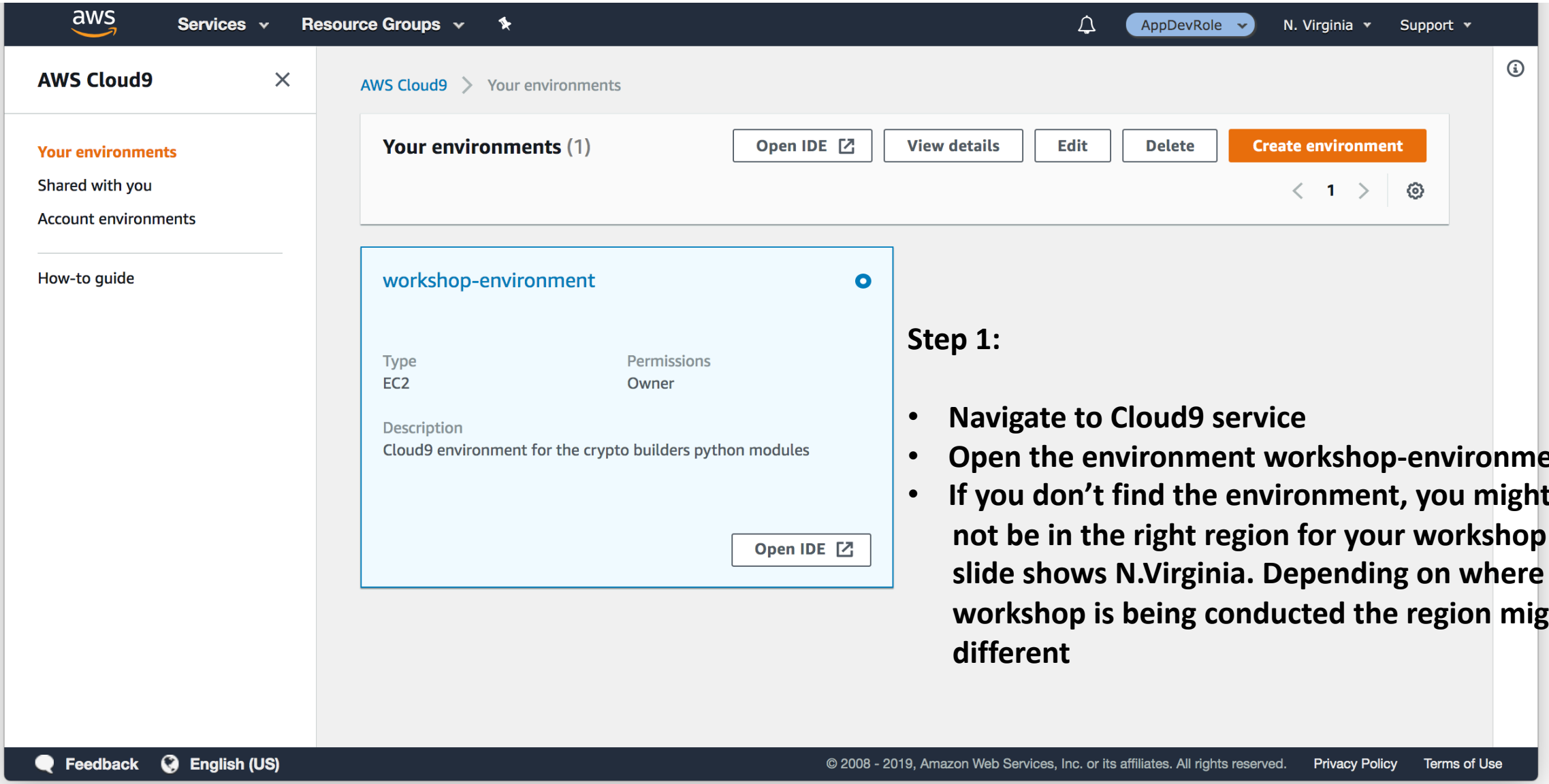
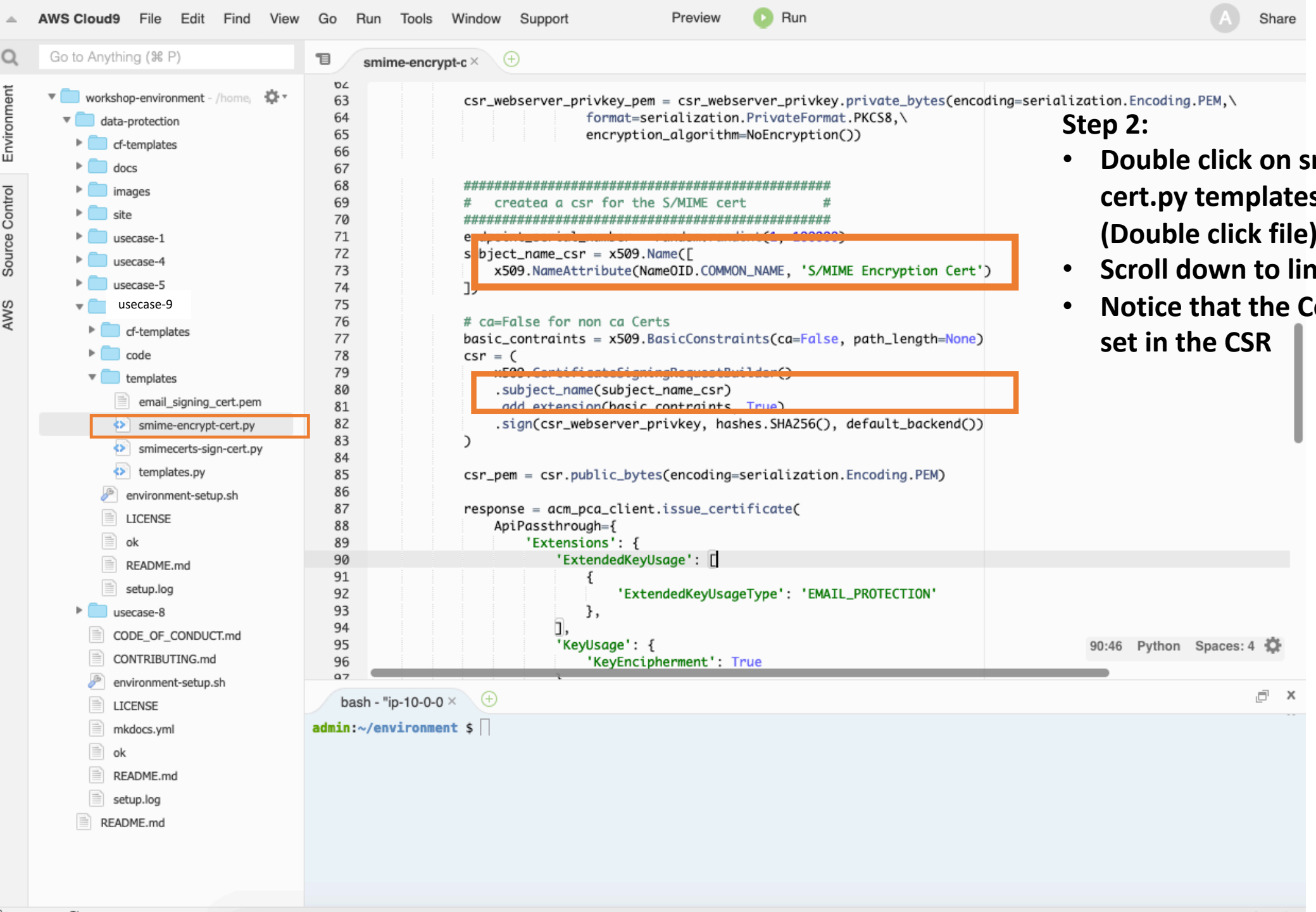


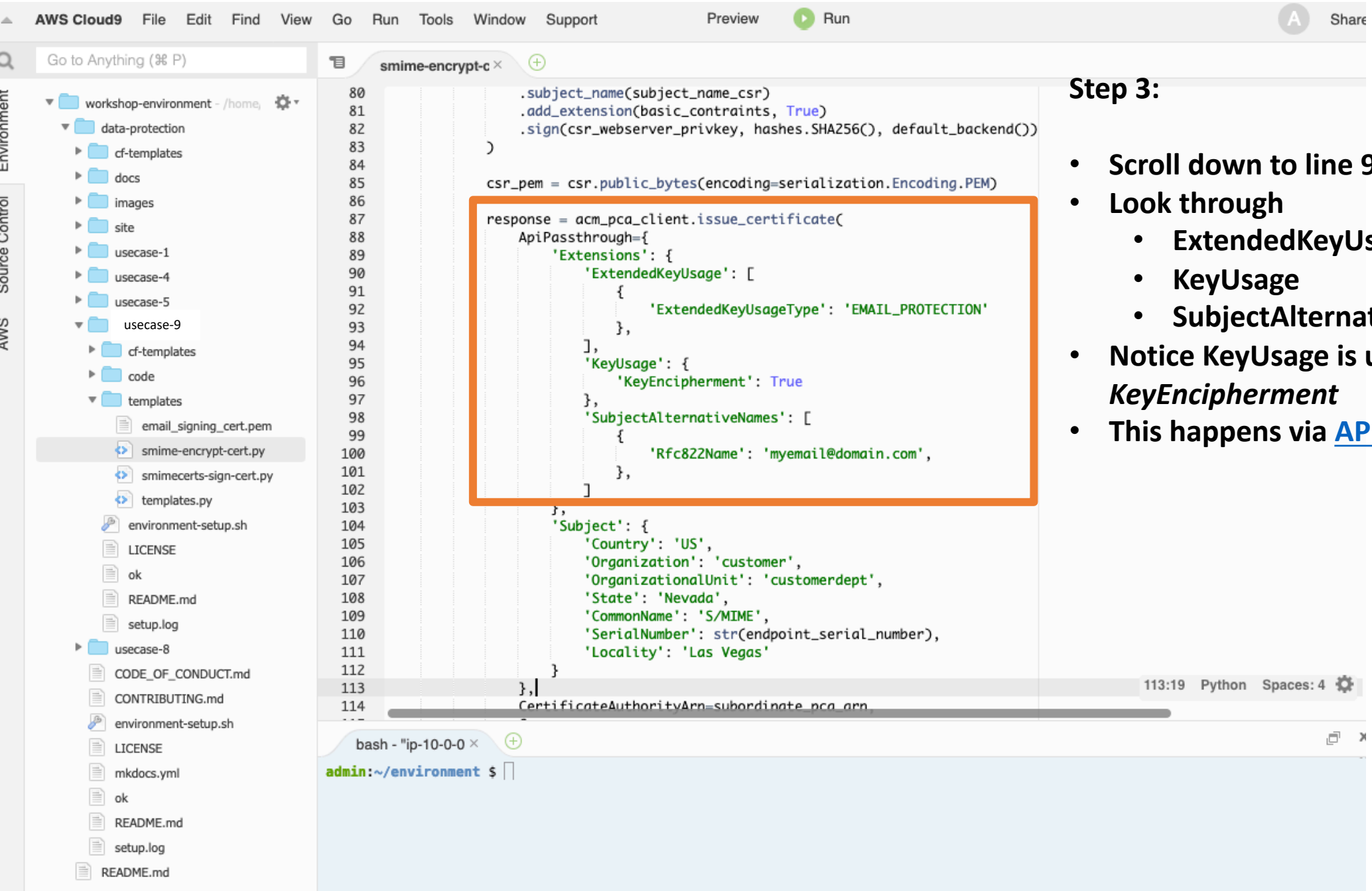
Step 1:

- **Navigate to Cloud9 service**
- **Open the environment workshop-environment**
- **If you don't find the environment, you might not be in the right region for your workshop – this slide shows N.Virginia. Depending on where this workshop is being conducted the region might be different**



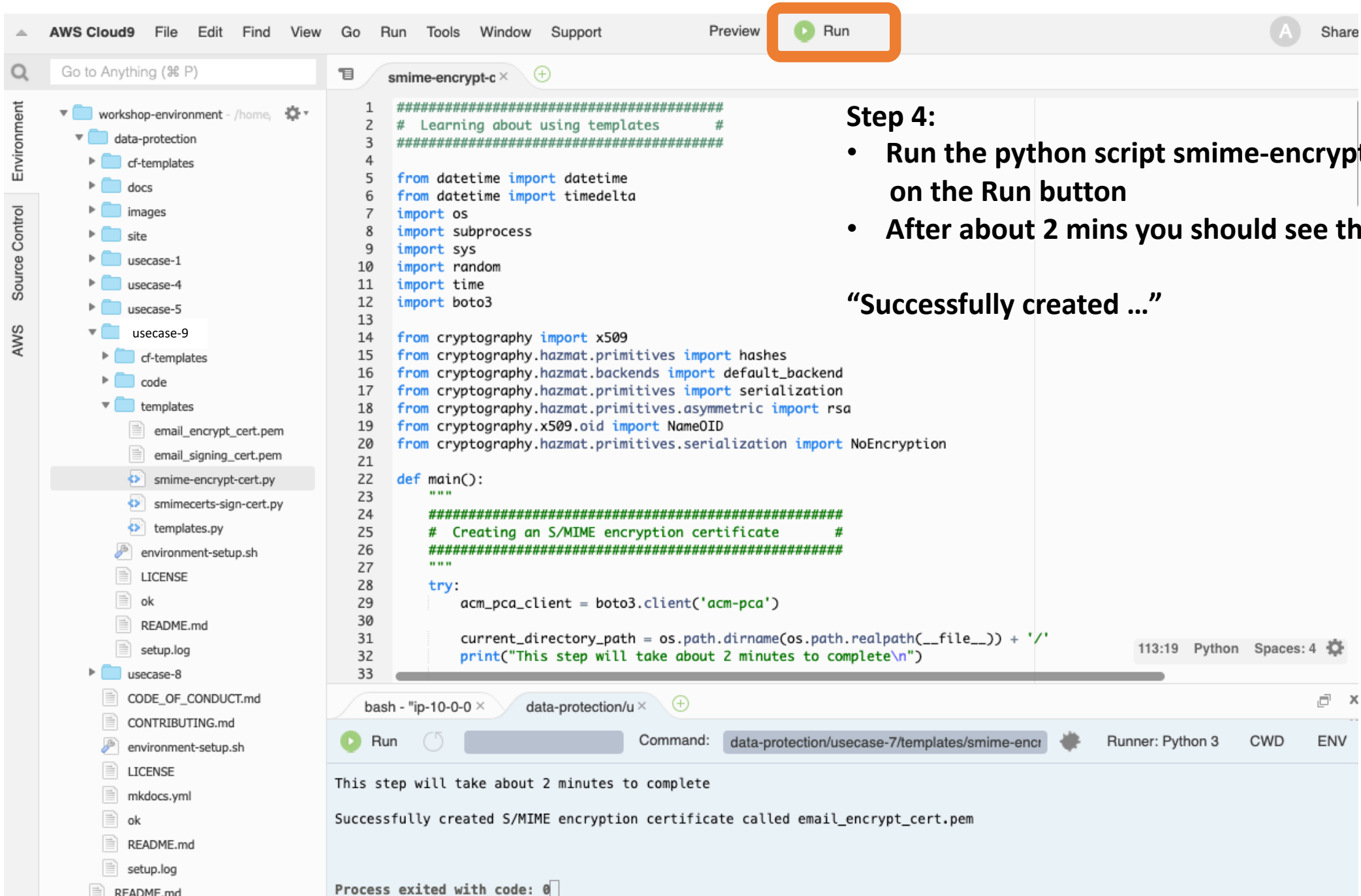
Step 2:

- Double click on smime-encrypt-cert.py templates sub directory (Double click file)
- Scroll down to line 71-83
- Notice that the Common Name is set in the CSR



Step 3:

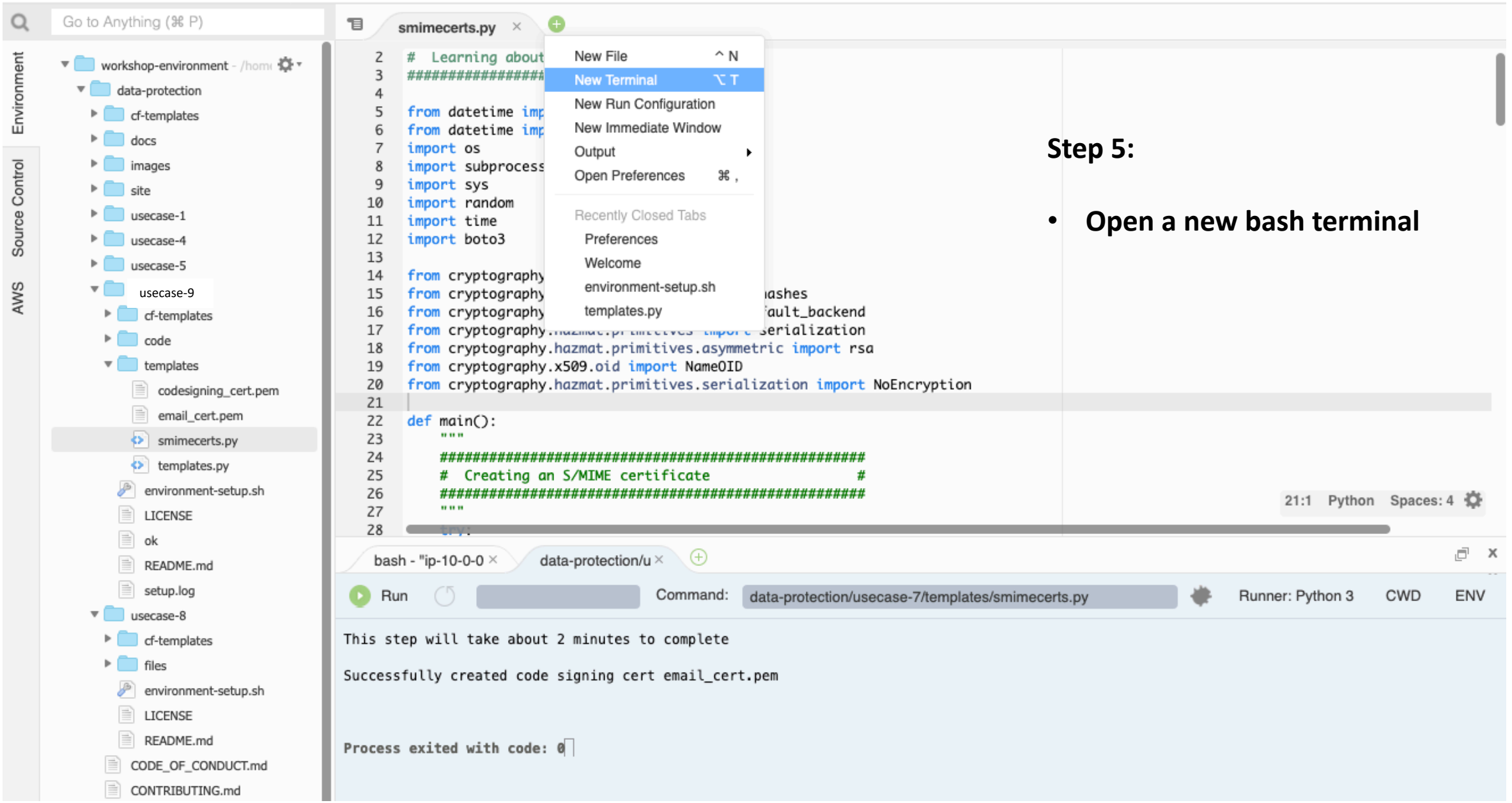
- **Scroll down to line 90**
- **Look through**
  - **ExtendedKeyUsage**
  - **KeyUsage**
  - **SubjectAlternativeNames**
- **Notice KeyUsage is using: *KeyEncipherment***
- **This happens via [API Passthrough]**



Step 4:

- **Run the python script smime-encrypt-cert.py by clicking on the Run button**
- **After about 2 mins you should see the print**

“Successfully created …”



Step 5:

- **Open a new bash terminal**

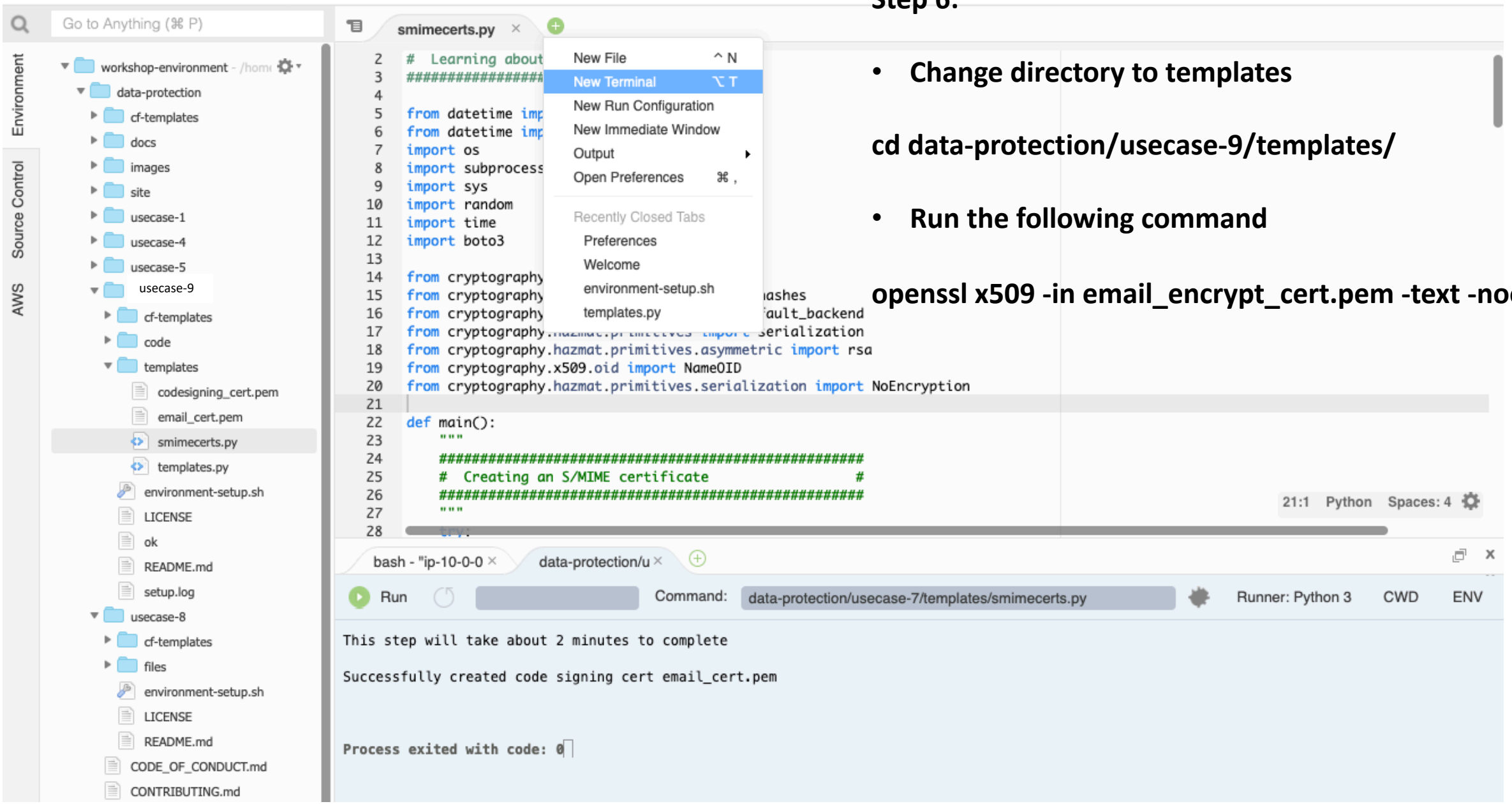
Step 6:

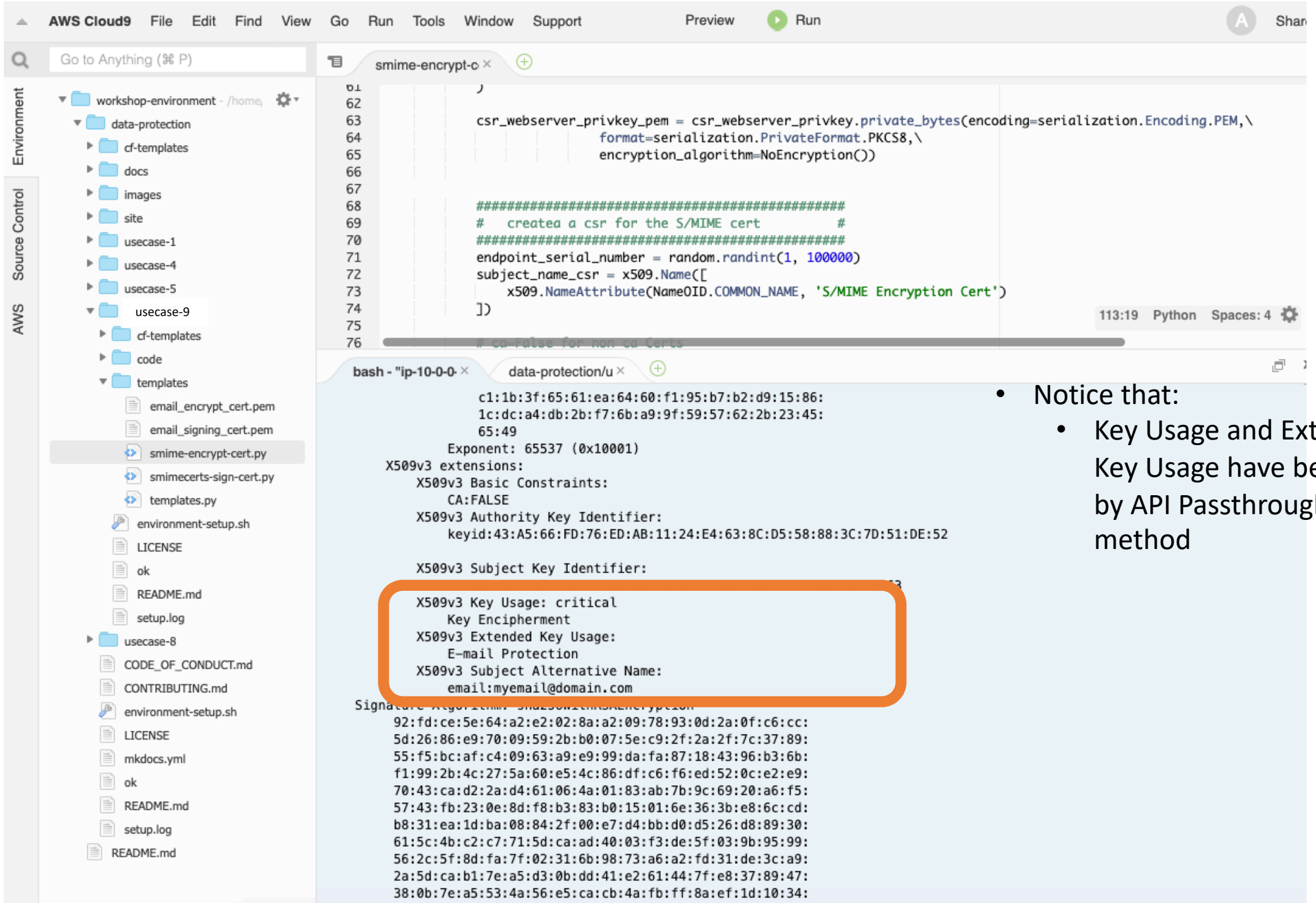
- **Change directory to templates**

cd data-protection/usecase-9/templates/

- **Run the following command**

openssl x509 -in email_encrypt_cert.pem -text -noout





- Notice that:
  - Key Usage and Extended Key Usage have been set by API Passthrough method