概述

对于需要客户端验证的场景，在Windows环境下，可以通过ADCS服务以及AD域策略实现Auto Enrollment 自动为用户注册客户端证书。但是如果用户环境里还有MacOS以及其他操作系统，并不能支持AD的自动颁发客户端证书的机制。所以这里提供了手动创建客户端证书的脚步，以及操作步骤，仅供参考。

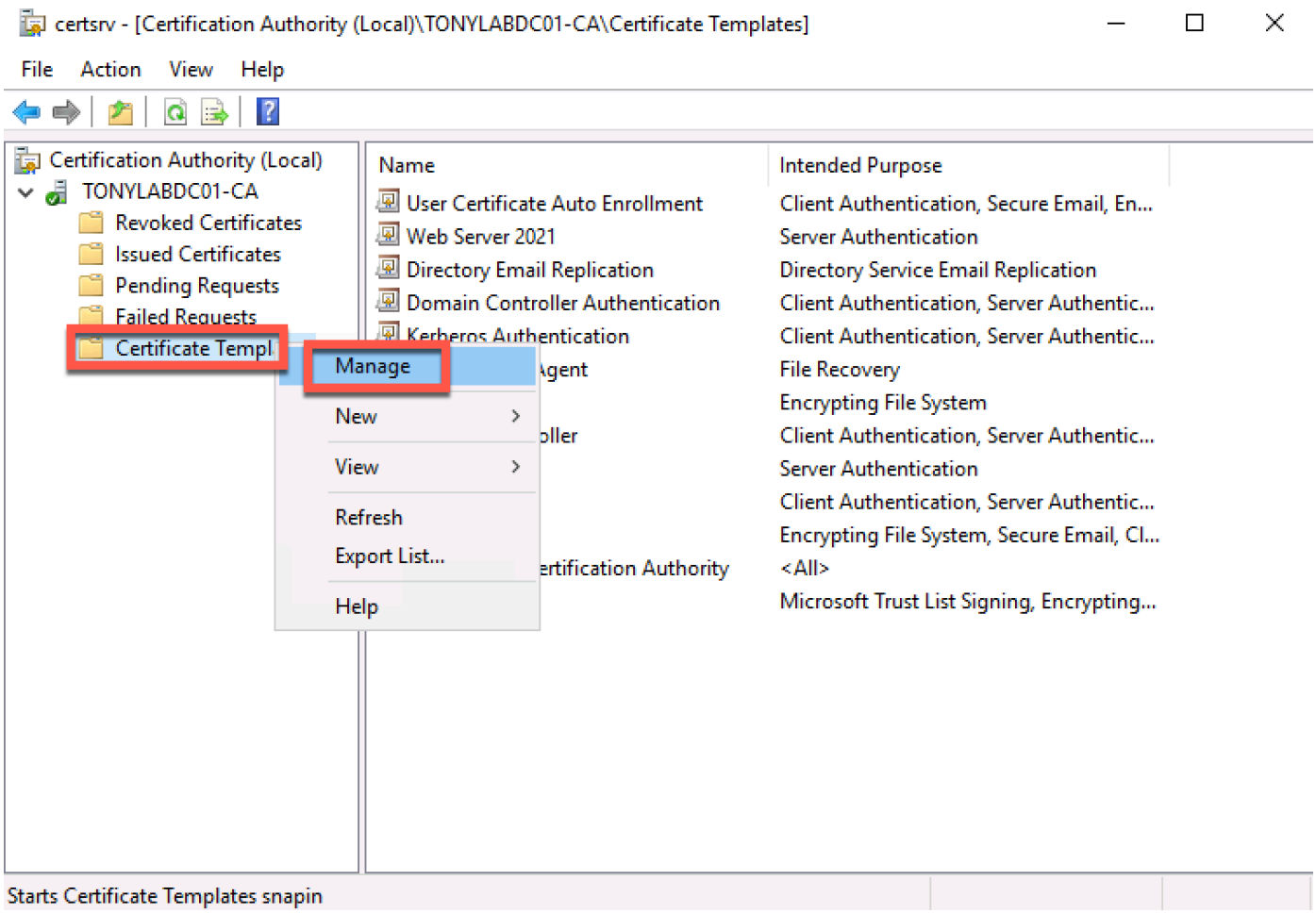
代码下载

Github 国内可能需要通过科学上网方式

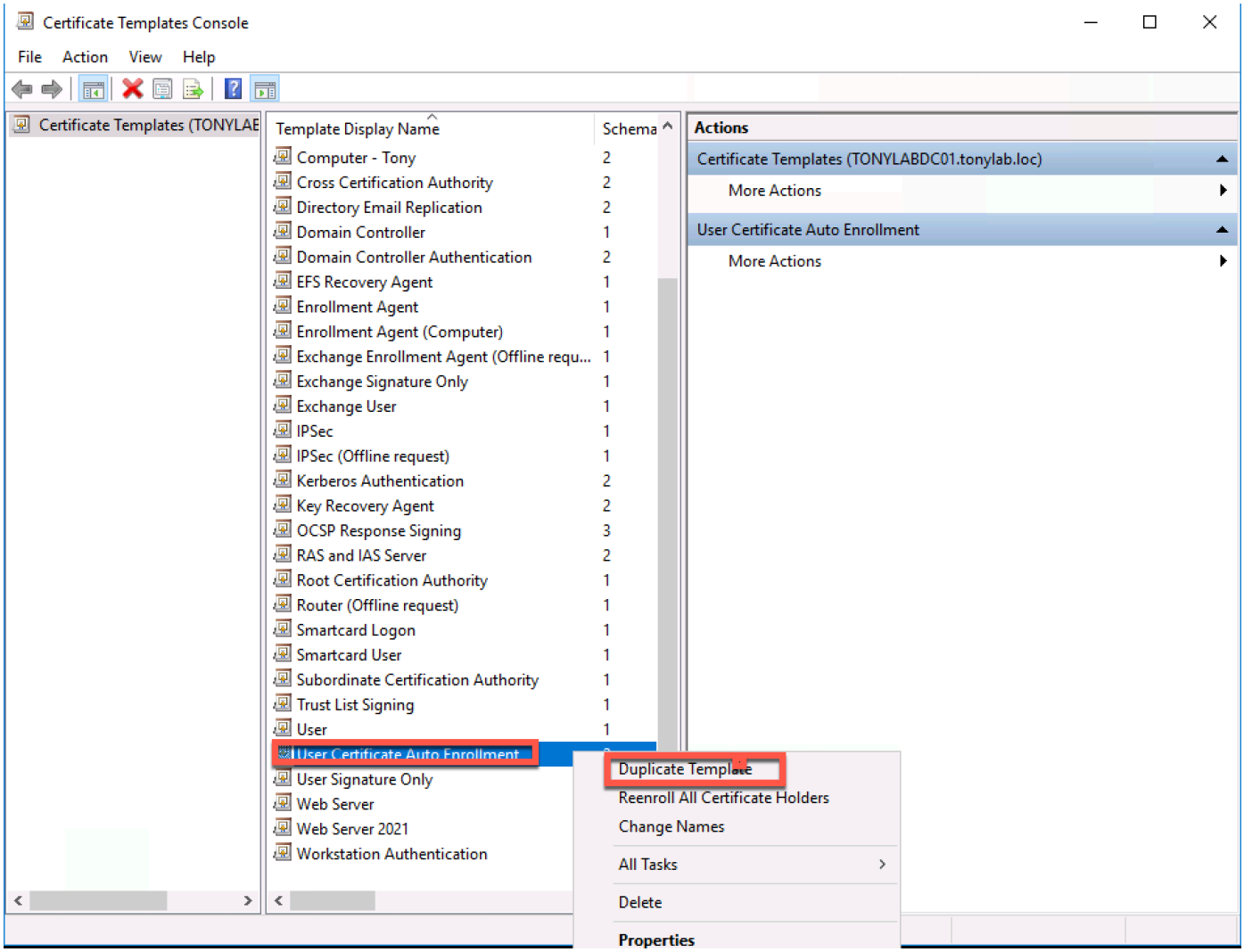
下载链接

操作步骤

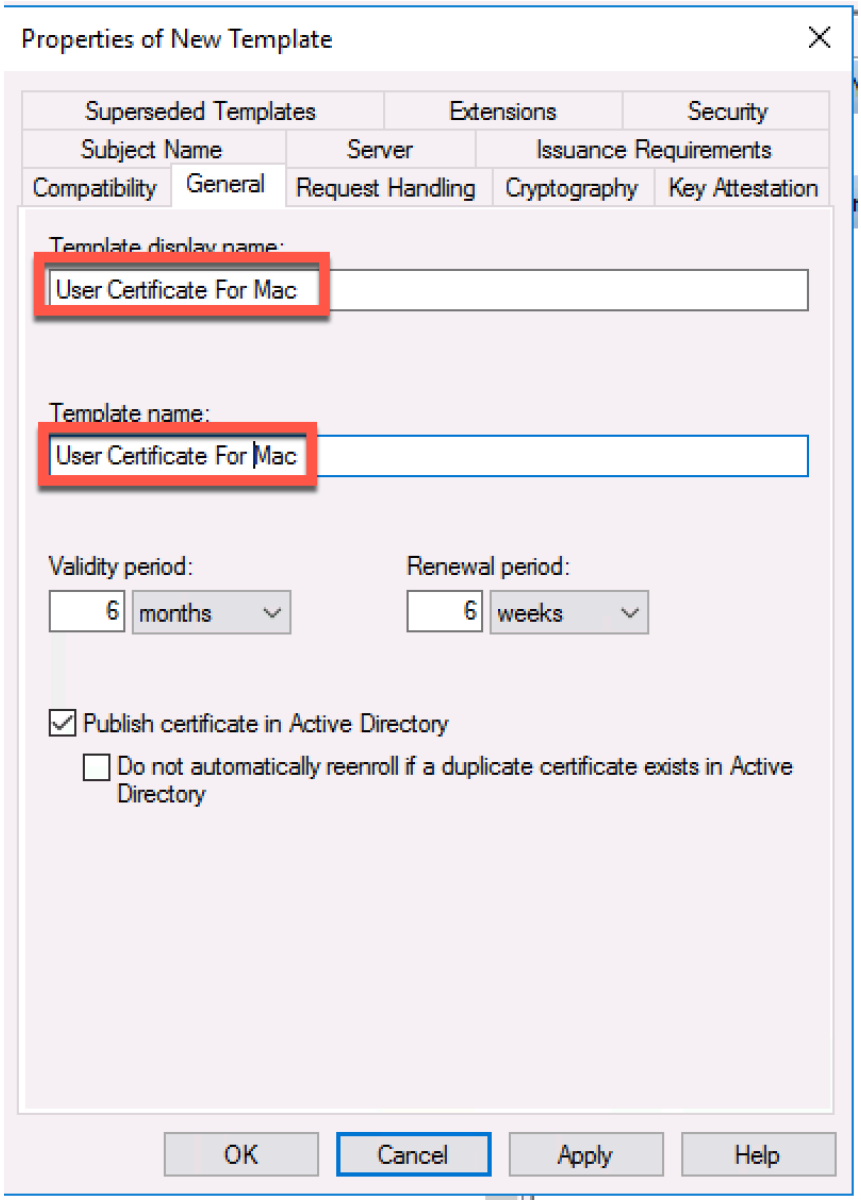
1. 打开 **Certificate Authority**, 选择 **Certificate Template** -> **Manage**



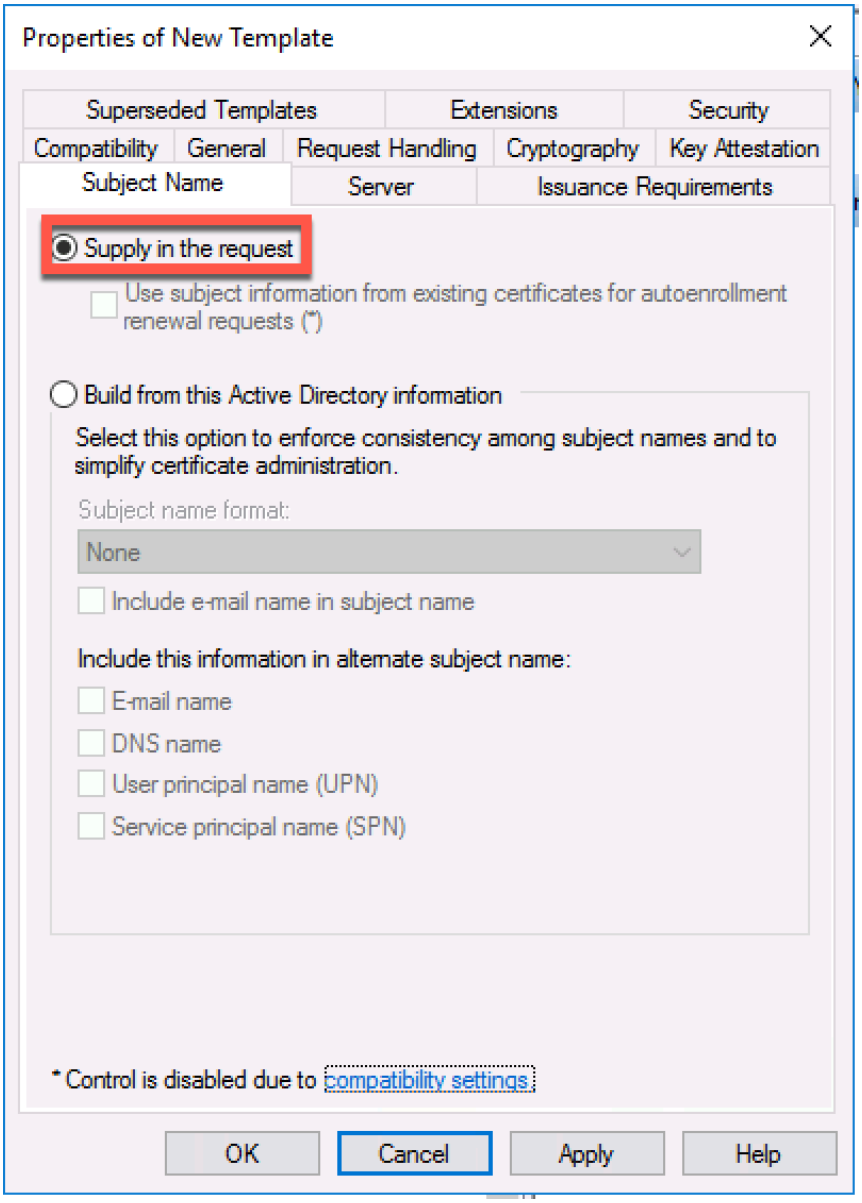
2. 选择之前创建的 **Cerififace Template** - **User Certificate Auto Enrollment** -> **Duplicate Template**



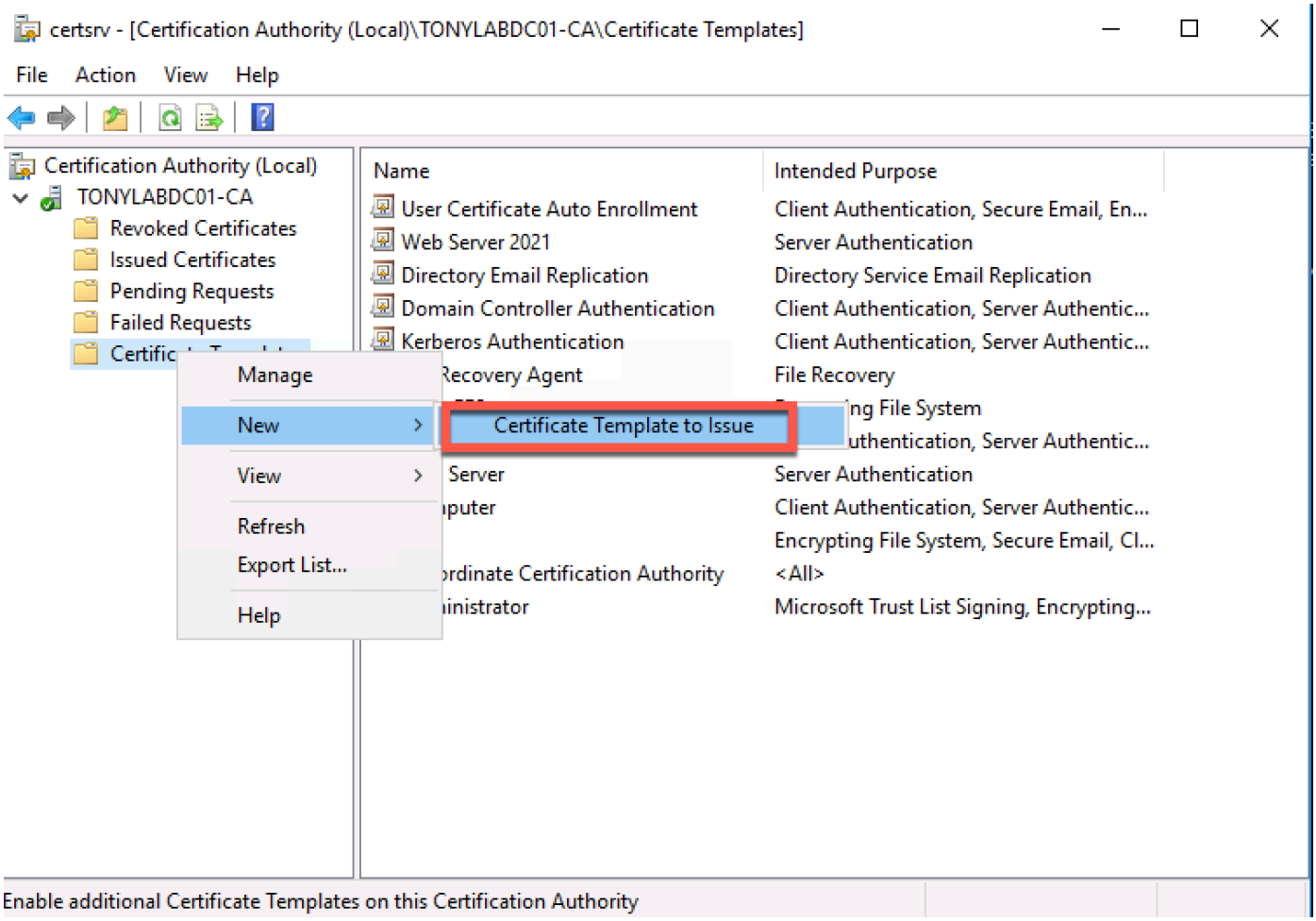
3. 修改 Template Name 为 **User Certificate For Mac**



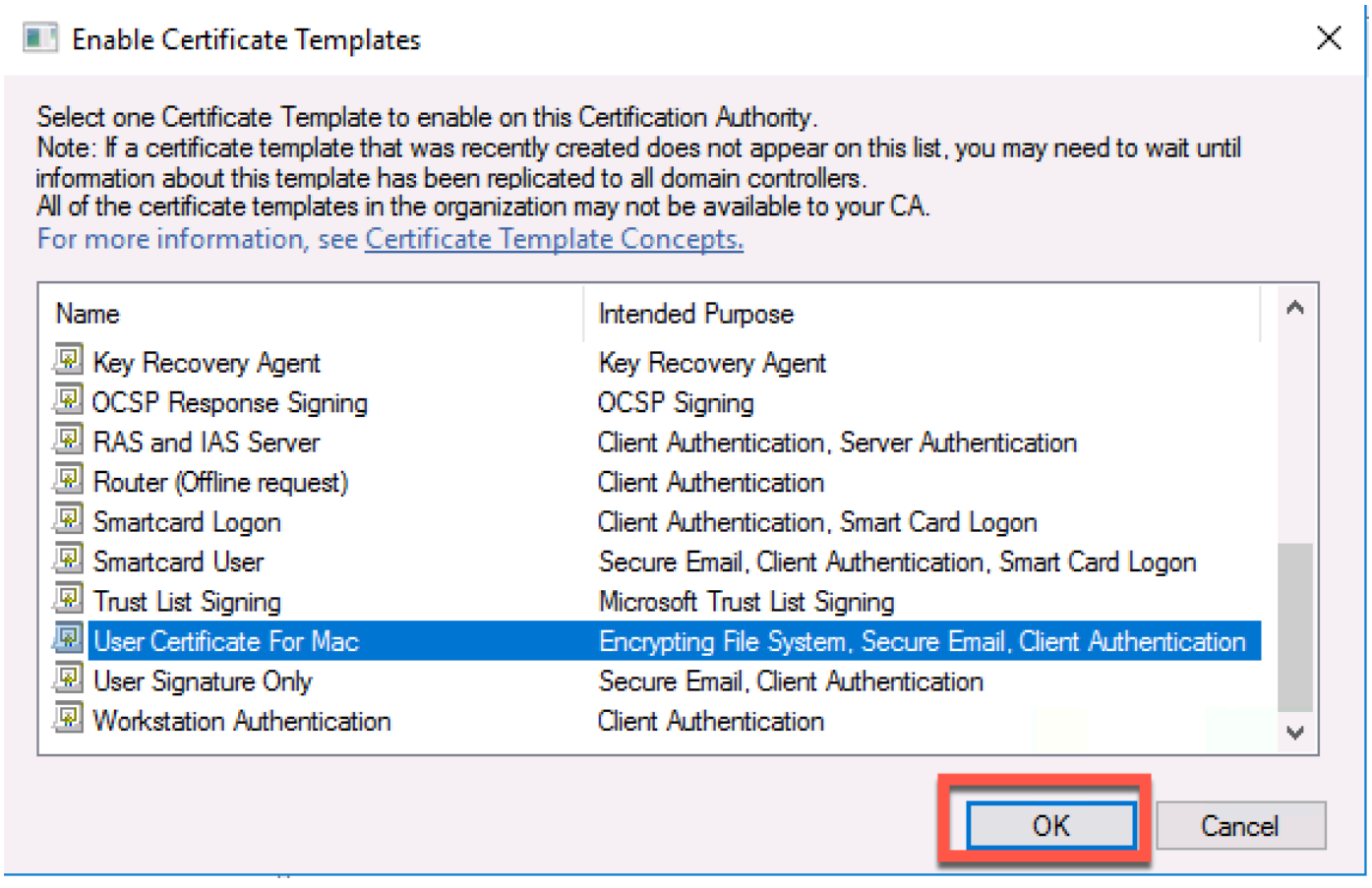
4. 选择 Subject Name 页面的设置 **Supply in the request**



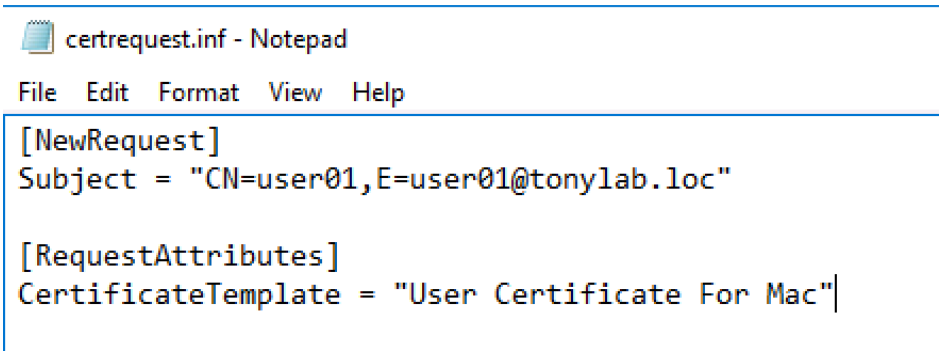
5. 回到 Certifiace Authority，选择 **New** -> **Certificate Template to Issue**



6. 选择 **User Certificate For Mac**，点击 **OK**



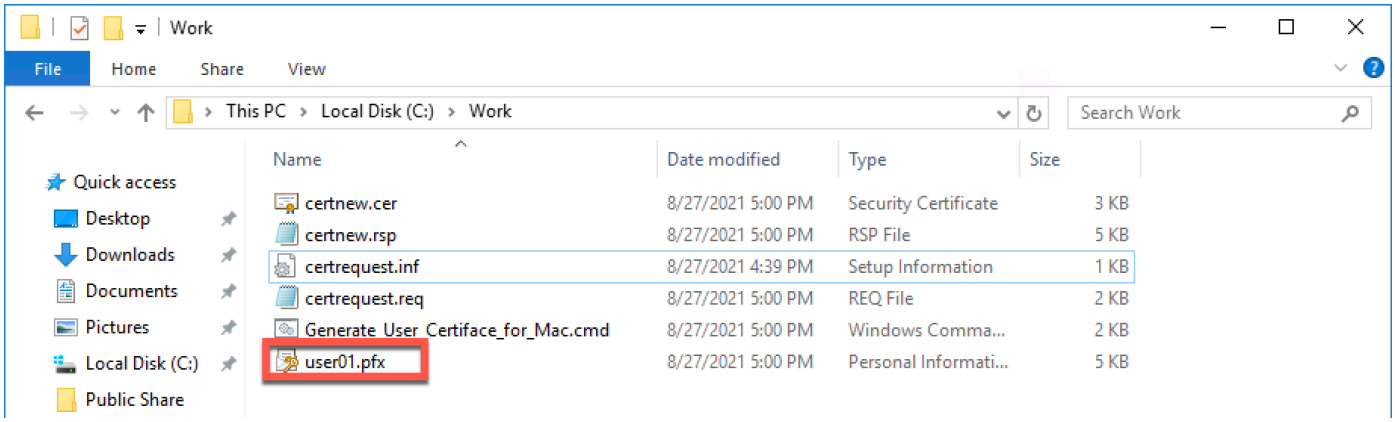
7. 修改** certrequest.inf** 文件，修改 **Subject 的用户名以及邮箱地址**



8. 执行 **Generate_User_Certiface_for_Mac.cmd** 脚本

```
c:\Work>Generate_User_Certiface_for_Mac.cmd

============  Created by Global Technology Integrator Co., Ltd. ==============================
Save the batch file "Generate_User_Certiface_for_Mac.cmd" and "certrequest.inf" to C:\Work
Modify C:\Work\certrequest.inf file accordingly.
This batch file will do the following:
1.    Create Certificate Request File
2.    Submit Certificate Request to CA and download the Certifiace
3.    Accept Certificate to Personal Folder and combind with private key
4.    Export PFX file that contains Certificate and Private Key.(PW:1q2w3e4r)
5.    Remove the Certificate from the local Personal Store
================================================================================================

Active Directory Enrollment Policy
  {226437A8-69F3-4A94-8EAD-666AC29CF950}
  ldap:

CertReq: Request Created
RequestId: 45
RequestId: "45"
Certificate retrieved(Issued) Issued
MY "Personal"
================ Certificate 1 ================
Serial Number: 5b0000002de2054da73a078a6a00000000002d
Issuer: CN=TONYLABDC01-CA, DC=tonylab, DC=loc
 NotBefore: 8/27/2021 4:50 PM
 NotAfter: 2/23/2022 4:50 PM
Subject: E=user01@tonylab.loc, CN=user01
Non-root Certificate
Template: User Certificate For Mac
Cert Hash(sha1): e6d965bd0e2e6f2f2edf08bf522ddf97f0aef2da
  Key Container = 53800869b9291a34a721ac24d6cf1a38_1c3b4cab-5c30-412e-b8b3-86edb3202376
  Simple container name: tq-User Certificate For Mac-89885116-8ed7-4131-a232-1c887a069834
  Provider = Microsoft Enhanced Cryptographic Provider v1.0
Microsoft Enhanced Cryptographic Provider v1.0: KeySpec=1
AES256+RSAES_OAEP(RSA:AT_KEYEXCHANGE) test passed
Encryption test passed
Signature test passed
Microsoft Enhanced Cryptographic Provider v1.0: KeySpec=1
AES256+RSAES_OAEP(RSA:CNG) test passed
Encryption test passed (CNG)
Signature test passed (CNG)
CertUtil: -exportPFX command completed successfully.
MY "Personal"
Deleting Certificate 1: E=user01@tonylab.loc, CN=user01:e6d965bd0e2e6f2f2edf08bf522ddf97f0aef2da
CertUtil: -delstore command completed successfully.

c:\Work>
```

9. 生成了用户名 - **user01.pfx** 的证书文件



10. 登录 MacOS，拷贝user01.pfx 到本地，双击执行该文件，选择钥匙串为 - **登陆**，点击 **添加**

11. 输入密码 ，点击 **好**