客户端证书导入操作手册

安全须知

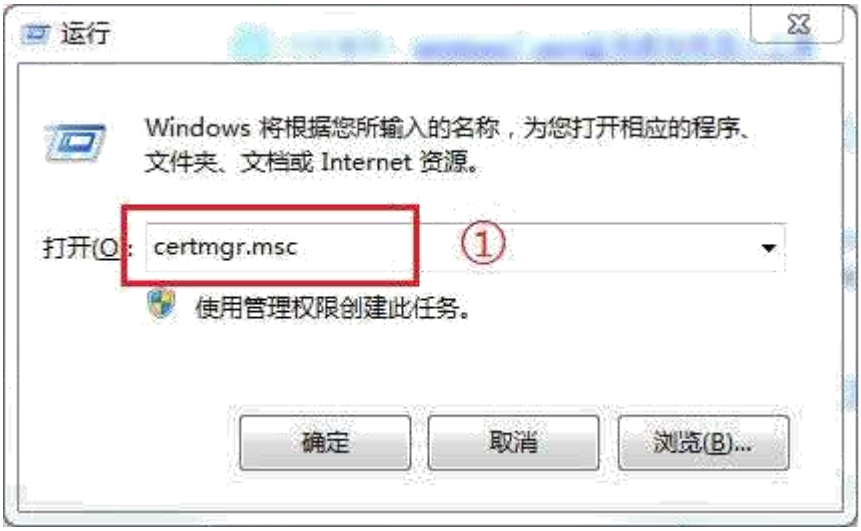
- **不要为操作系统或者浏览器导入任何其它根证书或者二级证书**
- **不要把自己的证书给他人使用**
- **按本文操作时，请核对 SHA1 指纹**
- **证书导入完毕后，请删除所有证书文件**

个人电脑

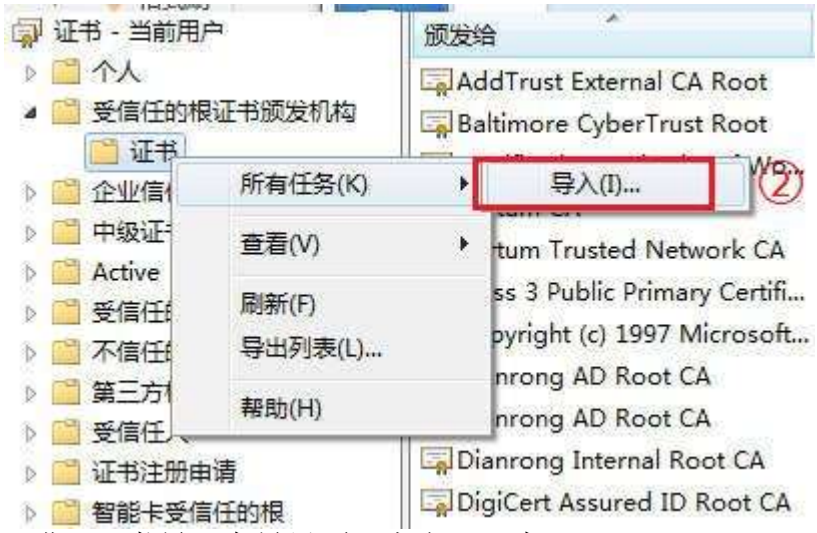
Windows 系统证书导入

一．导入 CA 根证书

1．在运行中输入 certmgr.msc,打开证书管理控制台



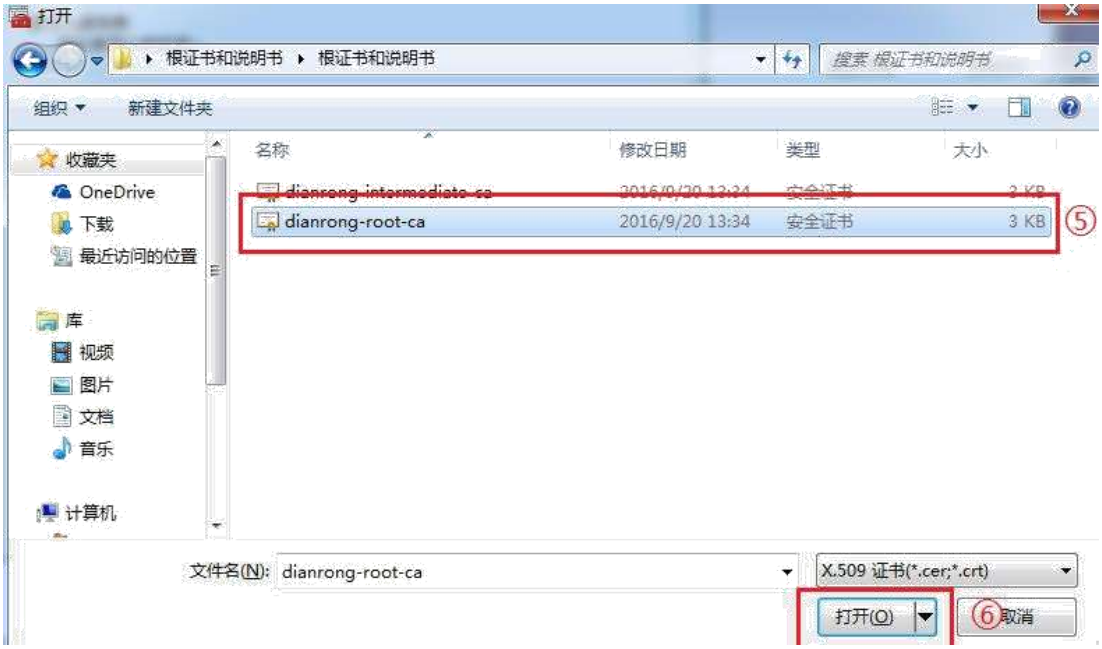
2.选择受信任的根证书颁发机构\证书，右击所有任务→导入



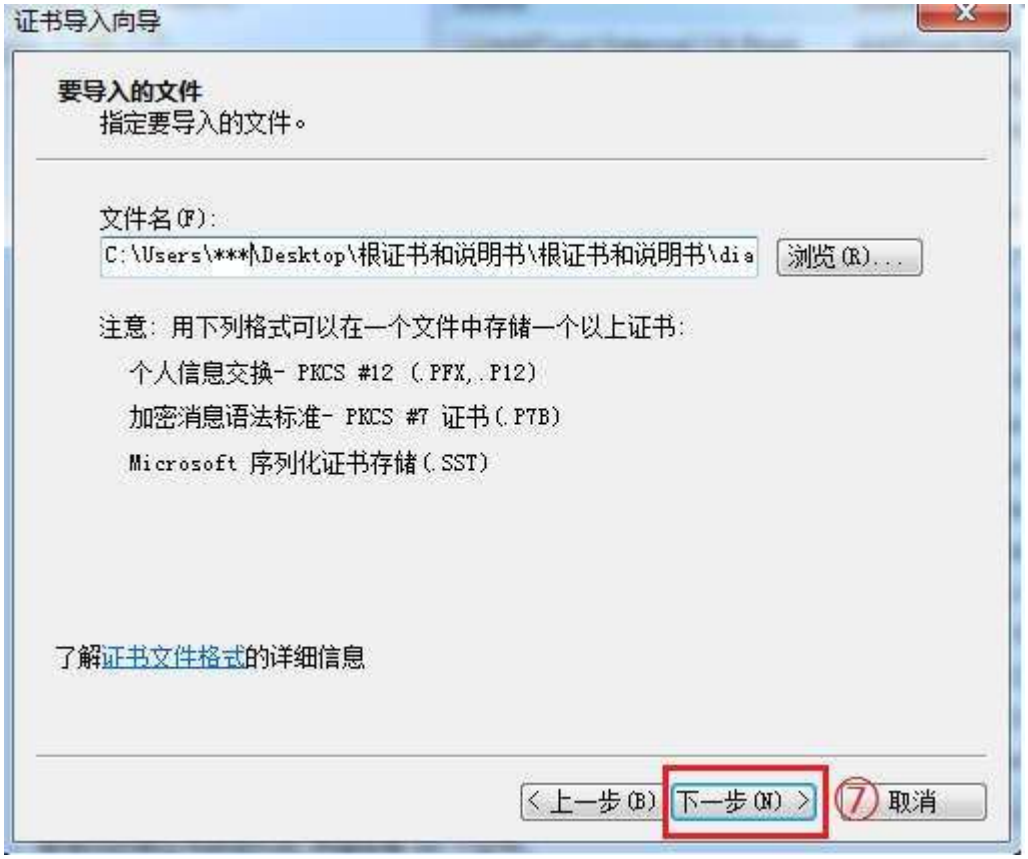
3 进入证书导入向导界面，点击下一步

t

4.点击浏览，在文件目录中选择 CA 根证书，点击打开→下一步



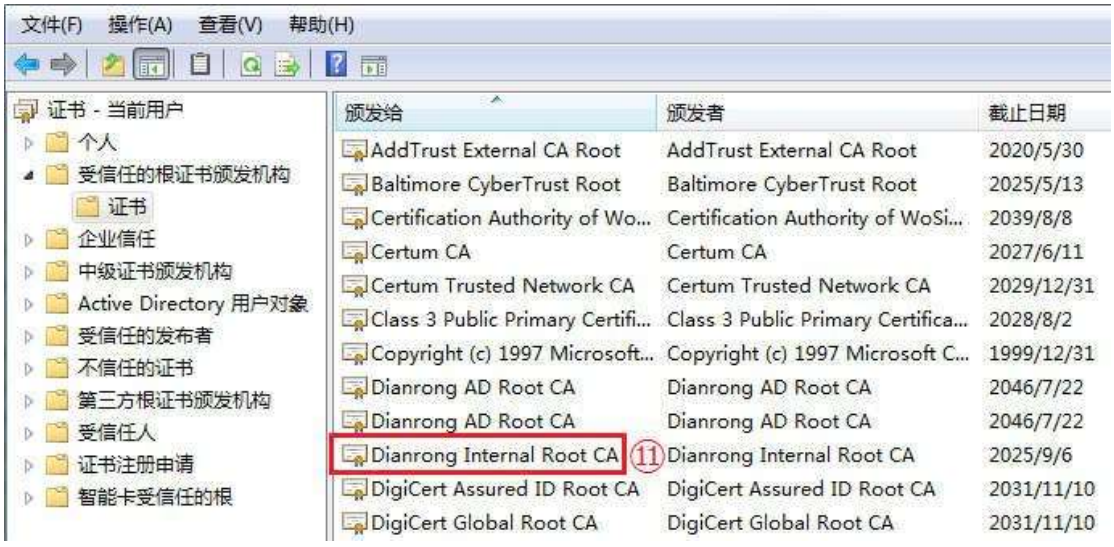
5.保持默认选项，点击下一步



6.点击完成，点击是安装证书

核对 sha1 指纹，无误点击是

7.导入成功,在右侧可以查看到 CA 根证书，说明操作成功

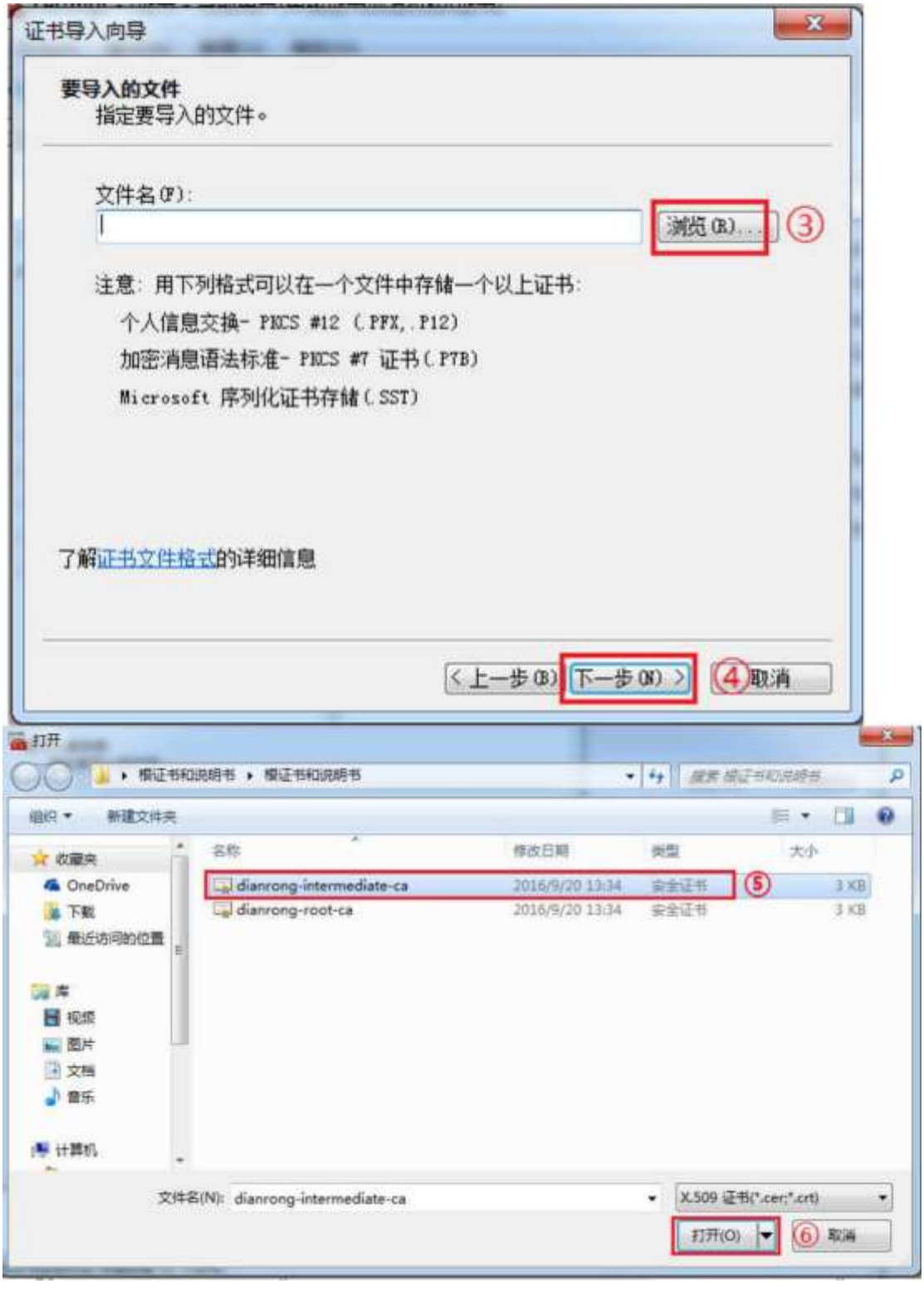


二．导入二级证书

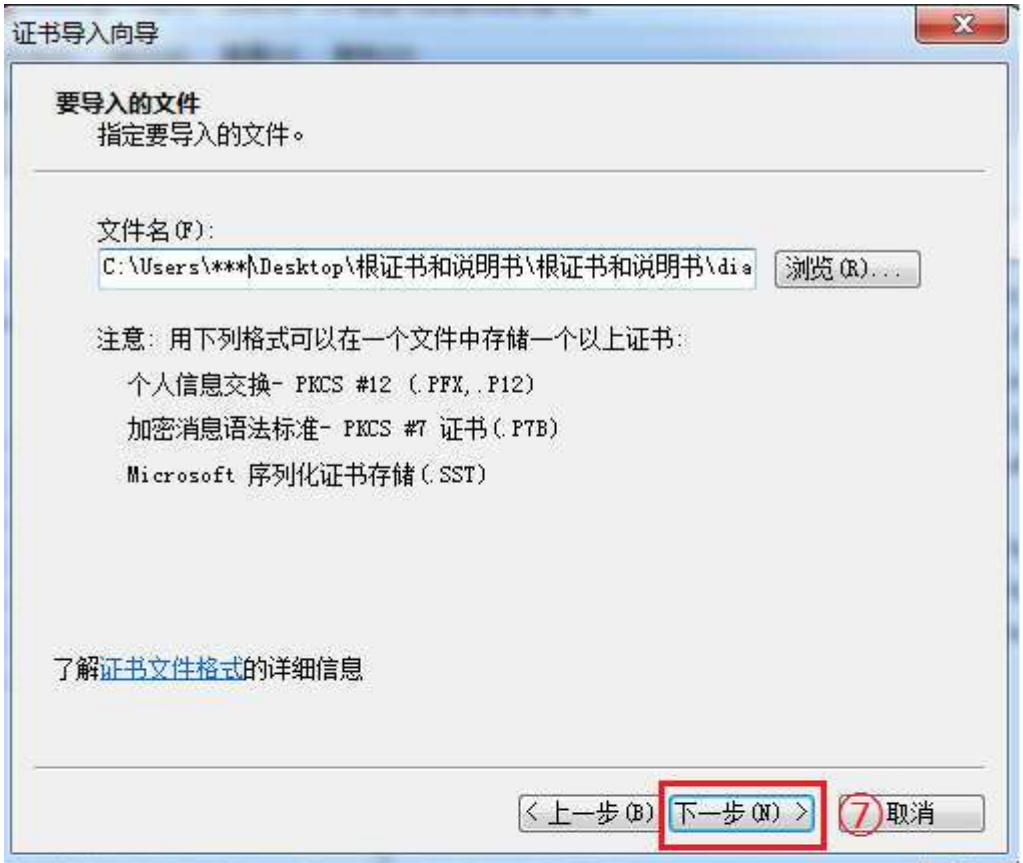
1. 选择中级证书颁发机构\证书, 右击所有任务→导入

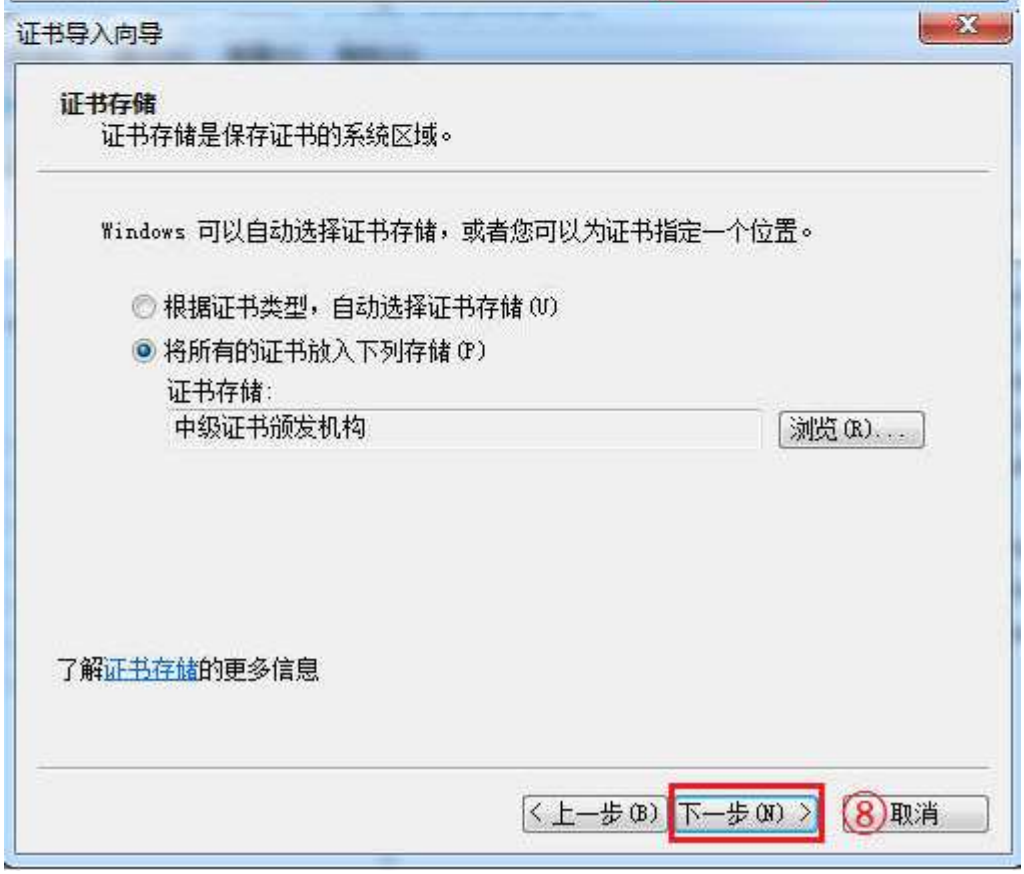
2. 进入证书导入向导界面，点击下一步

3.选择浏览，选择二级证书



4．保持默认选项，点击下一步，点击完成

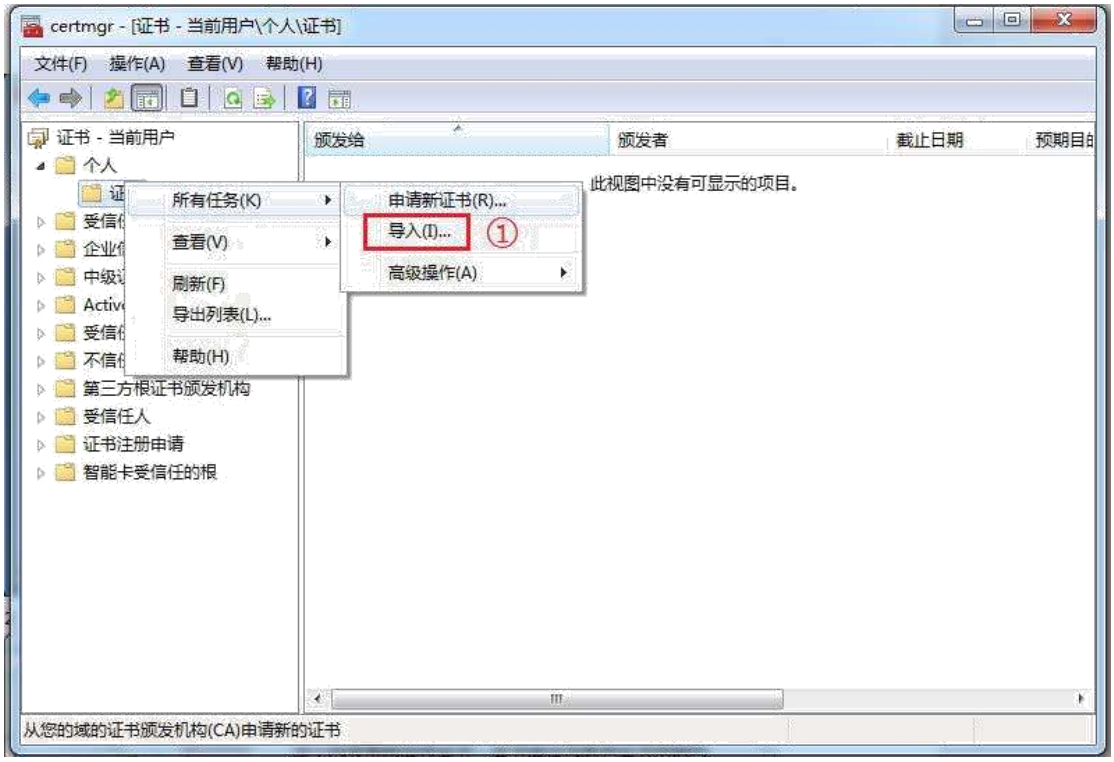

证书导入向导
要导入的文件
指定要导入的文件。
文件名(F):
C:\Users***\Desktop\根证书和说明书\根证书和说明书\dia
浏览(R)...
注意：用下列格式可以在一个文件中存储一个以上证书：
个人信息交换- PKCS #12 (.PFX,.P12)
加密消息语法标准- PKCS #7 证书(.P7B)
Microsoft 序列化证书存储(.SST)
了解证书文件格式的详细信息
< 上一步(B)
下一步(N) >
7
取消


证书导入向导
证书存储
证书存储是保存证书的系统区域。
Windows 可以自动选择证书存储，或者您可以为证书指定一个位置。
根据证书类型，自动选择证书存储(U)
将所有的证书放入下列存储(P)
证书存储:
中级证书颁发机构
浏览(R)...
了解证书存储的更多信息
< 上一步(B)
下一步(N) >
8
取消

5．导入成功，查看是否导入成功

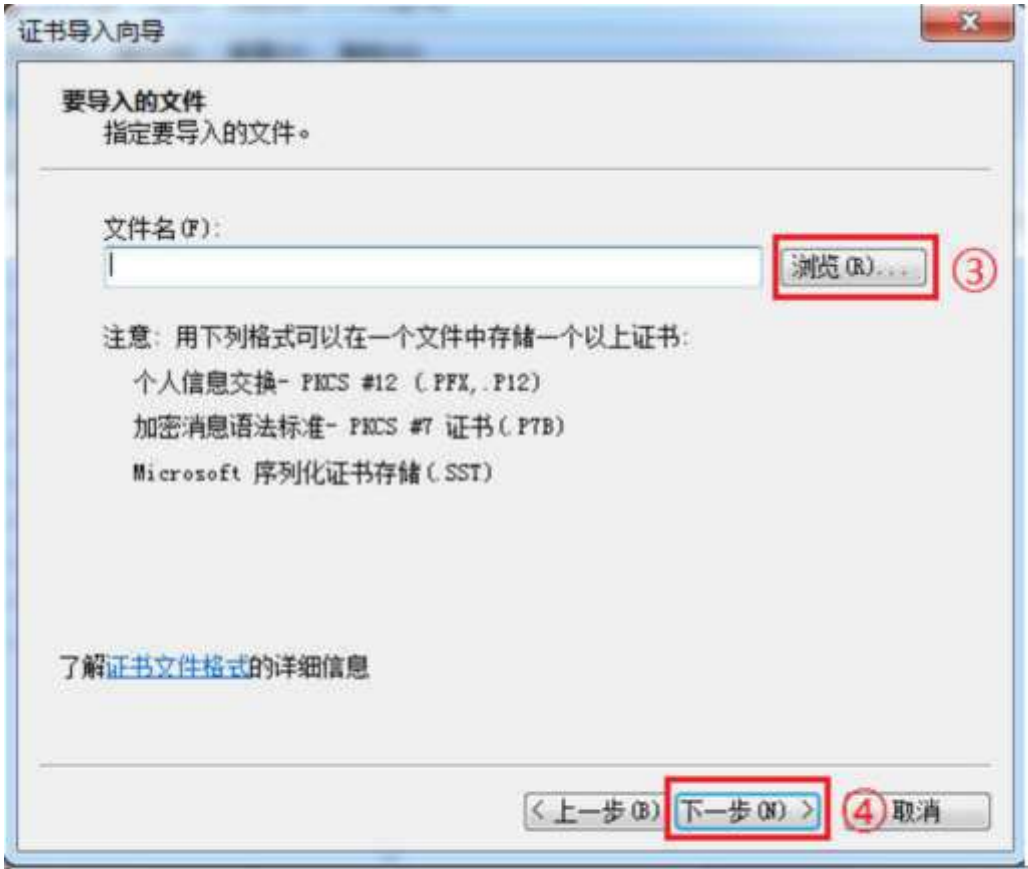
三．导入个人证书

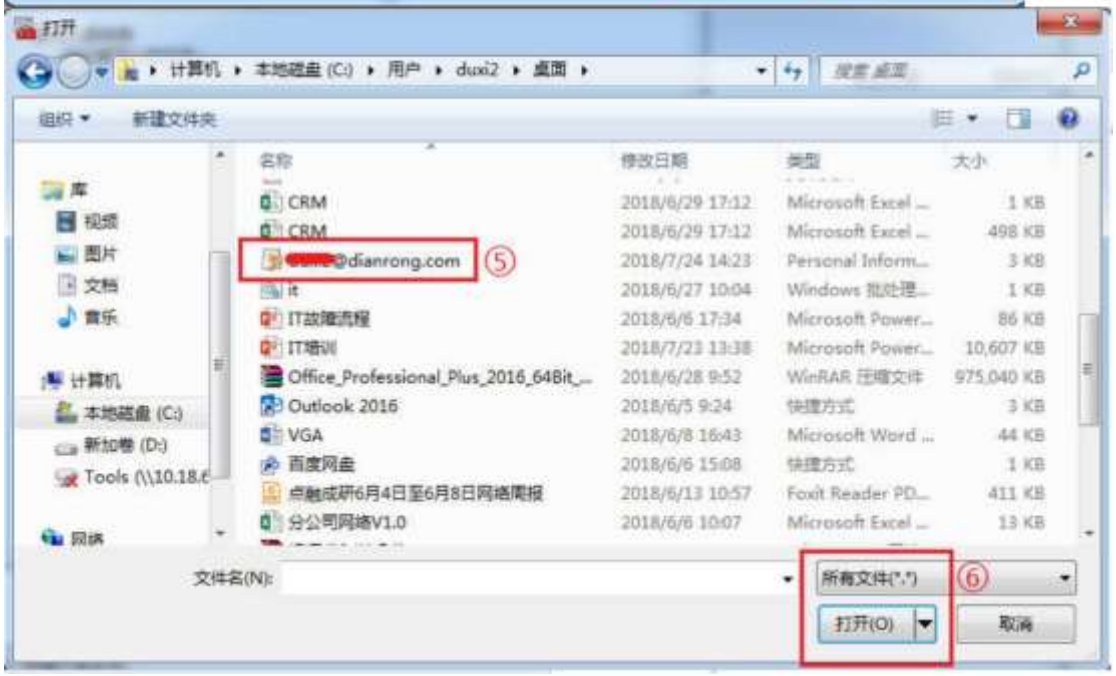
1．选择个人，右击所有任务→导入

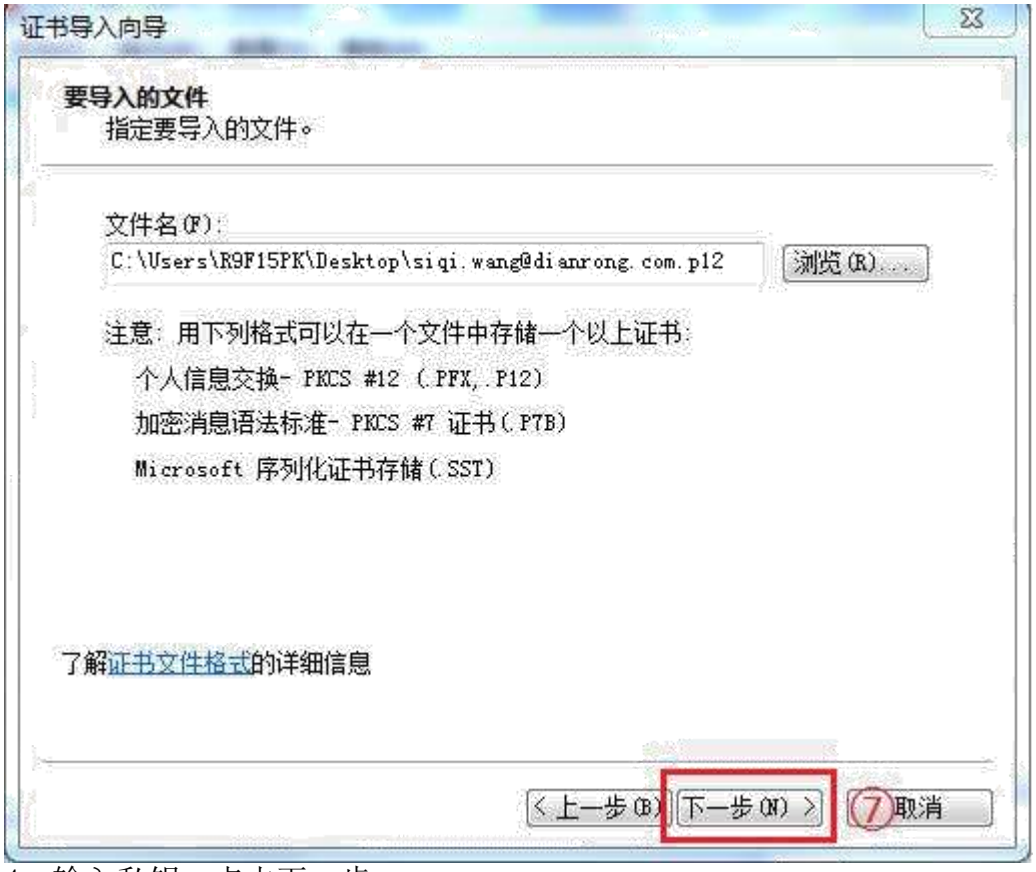


2．进入证书导入向导界面，点击下一步

3.选择浏览，选择个人证书，点击下一步


证书导入向导
要导入的文件
指定要导入的文件。
文件名(F):
浏览(R)...
③
注意：用下列格式可以在一个文件中存储一个以上证书：
个人信息交换- PKCS #12 (.PFX,.P12)
加密消息语法标准- PKCS #7 证书(.P7B)
Microsoft 序列化证书存储(.SST)
了解证书文件格式的详细信息
< 上一步(B)
下一步(N) >
④ 取消


打开
计算机 ▸ 本地磁盘 (C:) ▸ 用户 ▸ duxi2 ▸ 桌面 ▸
组织
新建文件夹
名称
修改日期
类型
大小
CRM
2018/6/29 17:12
Microsoft Excel ...
1 KB
CRM
2018/6/29 17:12
Microsoft Excel ...
498 KB
@dianrong.com
⑤
2018/7/24 14:23
Personal Inform...
3 KB
it
2018/6/27 10:04
Windows 批处理...
1 KB
IT故障流程
2018/6/6 17:34
Microsoft Power...
86 KB
IT培训
2018/7/23 13:38
Microsoft Power...
10,607 KB
Office_Professional_Plus_2016_64Bit_...
2018/6/28 9:52
WinRAR 压缩文件
975,040 KB
Outlook 2016
2018/6/5 9:24
快捷方式
3 KB
VGA
2018/6/8 16:43
Microsoft Word ...
44 KB
百度网盘
2018/6/6 15:08
快捷方式
1 KB
点触成研6月4日至6月8日网络简报
2018/6/13 10:57
Foxit Reader PD...
411 KB
分公司网络V1.0
2018/6/8 10:07
Microsoft Excel ...
13 KB
库
视频
图片
文档
音乐
计算机
本地磁盘 (C:)
新加卷 (D:)
网络
文件名(N):
所有文件(*.*)
⑥
打开(O)
取消

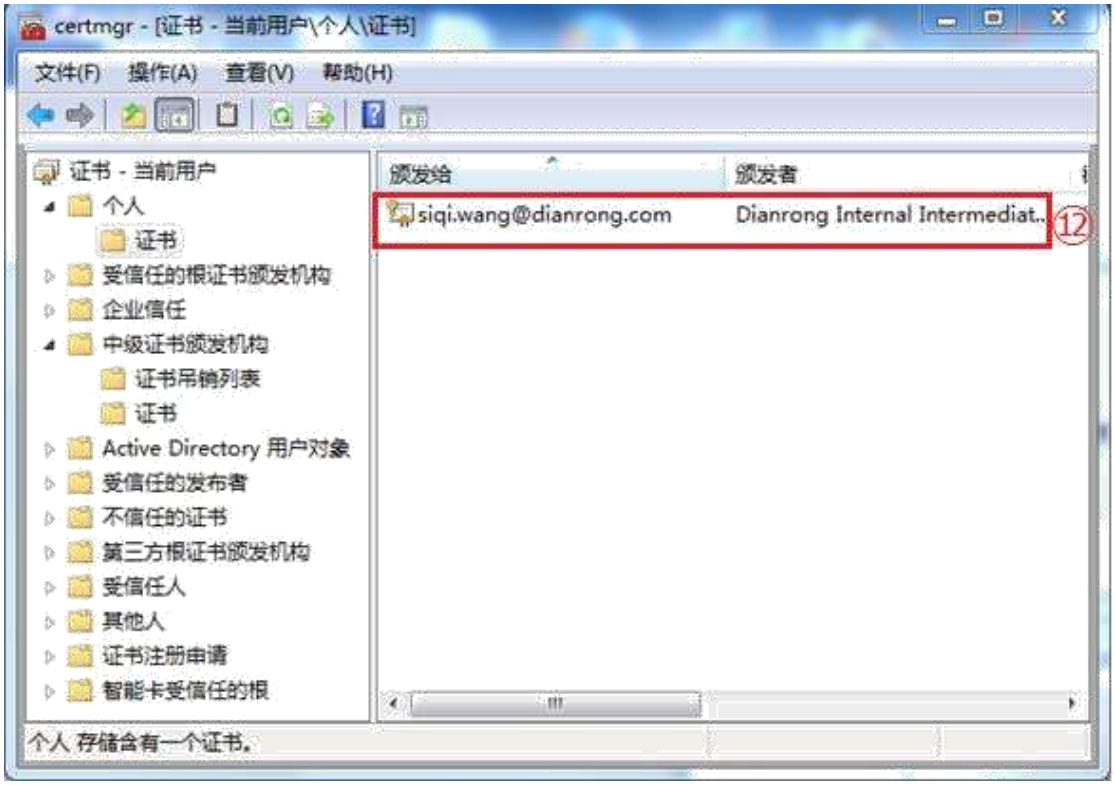


4．输入私钥，点击下一步

5．保持默认配置，点击下一步

6．点击完成

7．导入成功，查看是否导入成功



t

试连接应用或网站，证书是否生效，提供一个公司内部测试 URL：

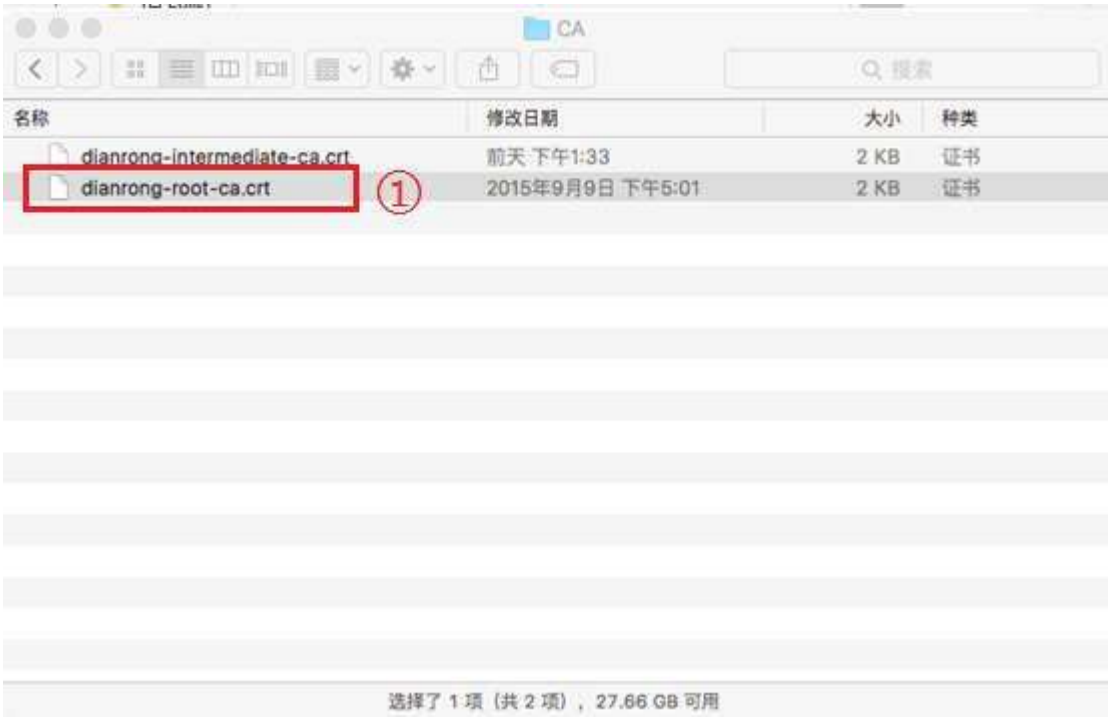
https://testcer.corp.dianrong.com

经过测试基本可以满足除了 Firefox 以外的浏览器的正常连接使用，
Firefox 配置请继续阅览下文

Mac OS X 系统证书导入

. 导入 CA 根证书

1. 双击 dianrong-root-ca.crt

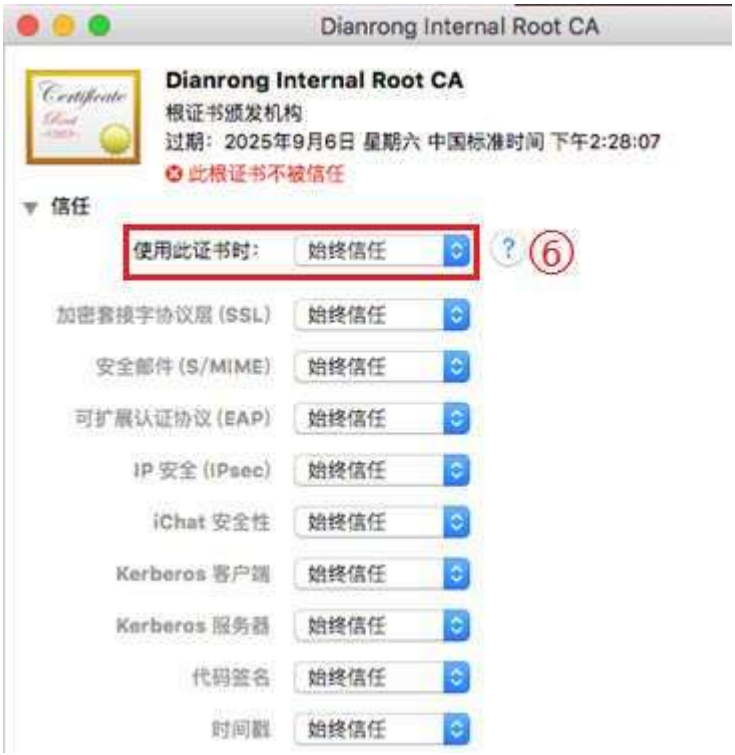


2.选择存位置为“系统”

3. 输入个人电脑密码

4. 系统会打开钥匙串访问，在搜索框中输入 dianrong，双击打开 Dianrong Internal Root CA

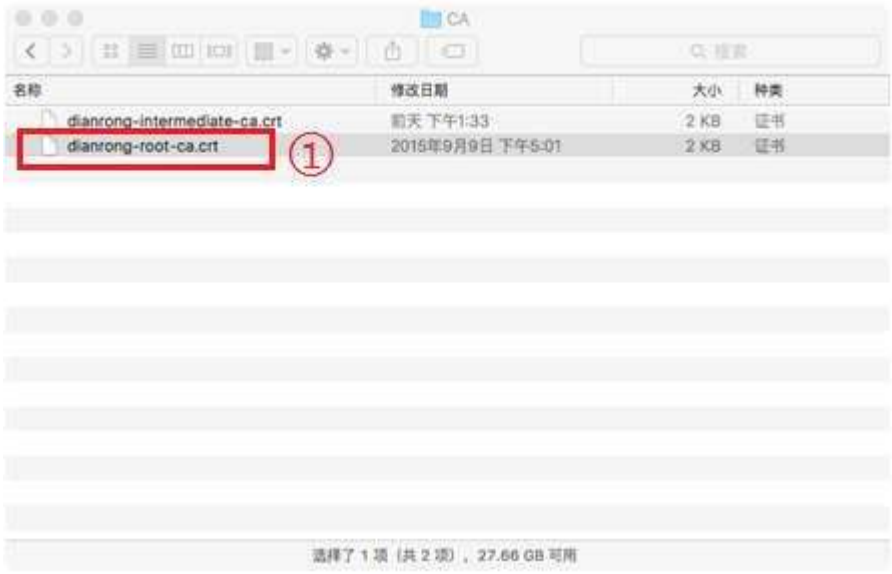
5. 使用此证书时：始终信任



6. 关闭窗口，输入密码

. 导入二级证书

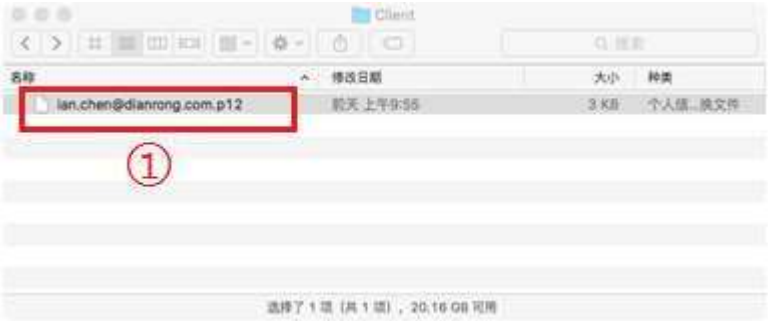
1. 双击证书导入



2. 打开钥匙串访问，在搜索框中输入 dianrong 。此时根证书显示信任，二级证书显示有效 。

三．导入个人证书

1. 双击个人证书



2. 输入证书密码（手机短信接收的证书密码）

3. 自动弹出证书导入窗口，请按照以下方式设置证书存放位置

4. 检查个人证书存放位置为“登录”下面

5个

用浏览器验证证书导入

浏览器 Chrome，Safari，IE 等均使用操作系统证书管理证书，不再需要对浏览器做任何设置。打开网址：https://uniauth.corp.dianrong.com/。以下截图以 Mac 平台的 Chrome 为例。

1.打开网址后，浏览器会要求访问钥匙串

2. 看到如下窗口，即表明所有证书导入成功。注意 https 这里必须是绿色的锁。

Firefox 浏览器证书配置

Firefox 使用自带的证书管理，必须单独配置。

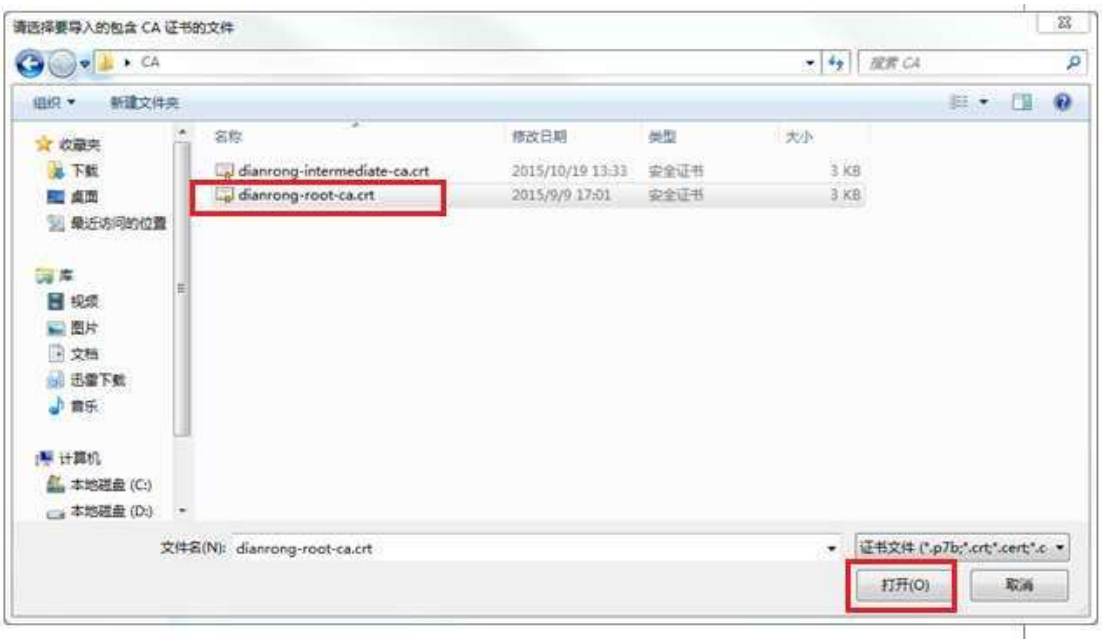
1．点击打开菜单，选择选项菜单

2．点击高级，选择证书项，点击查看证书

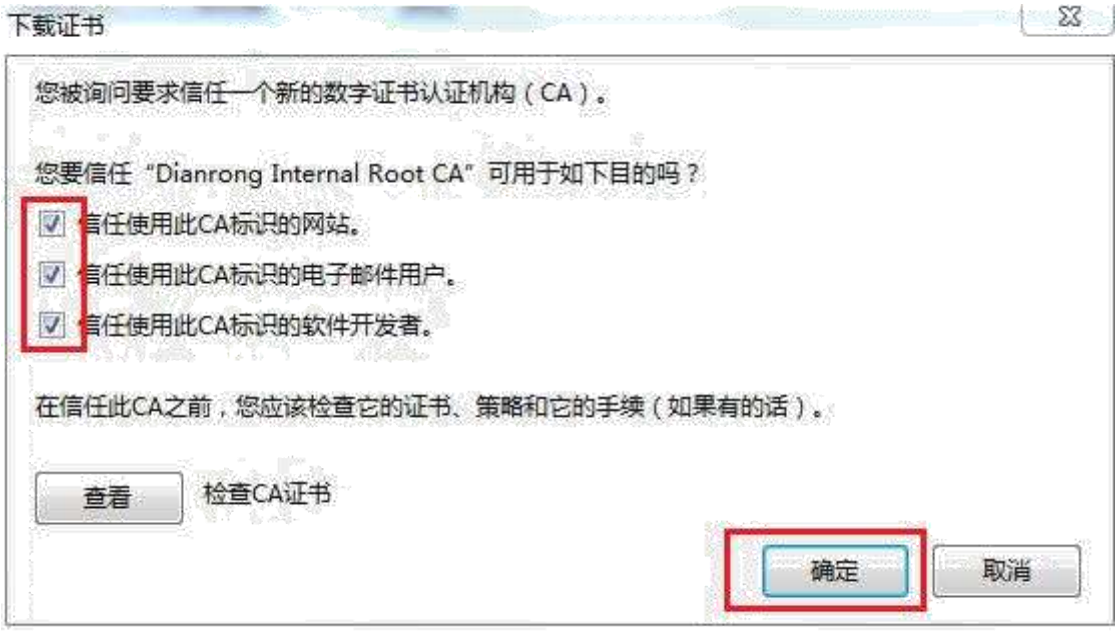
3．选择证书机构项，点击导入

t

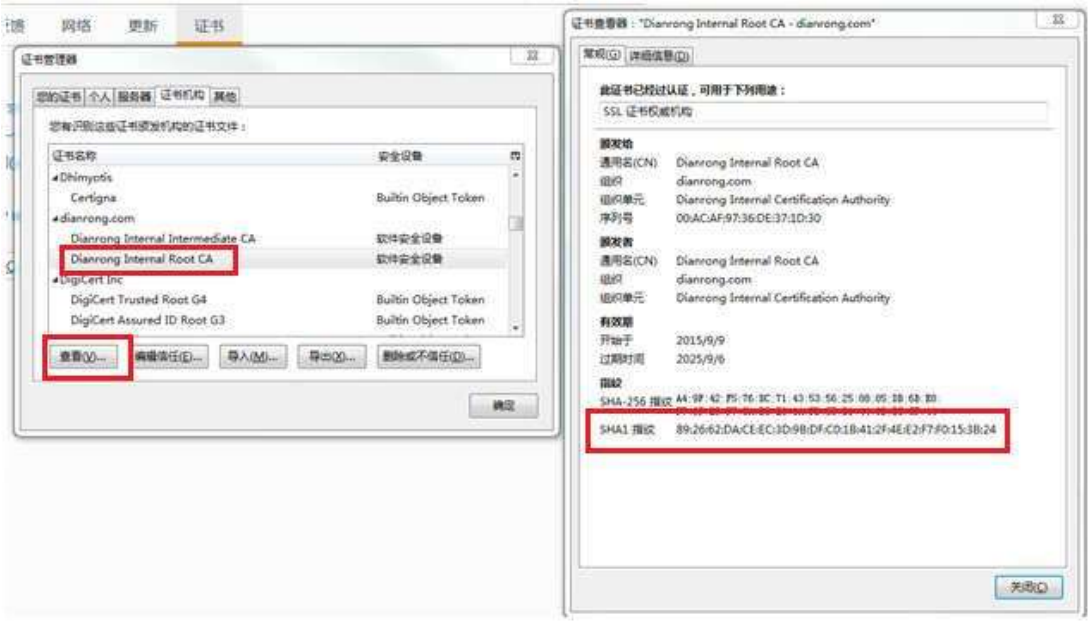
4．选择根证书，点击打开



5．对该证书配置信任，建议全部勾选，点击确定

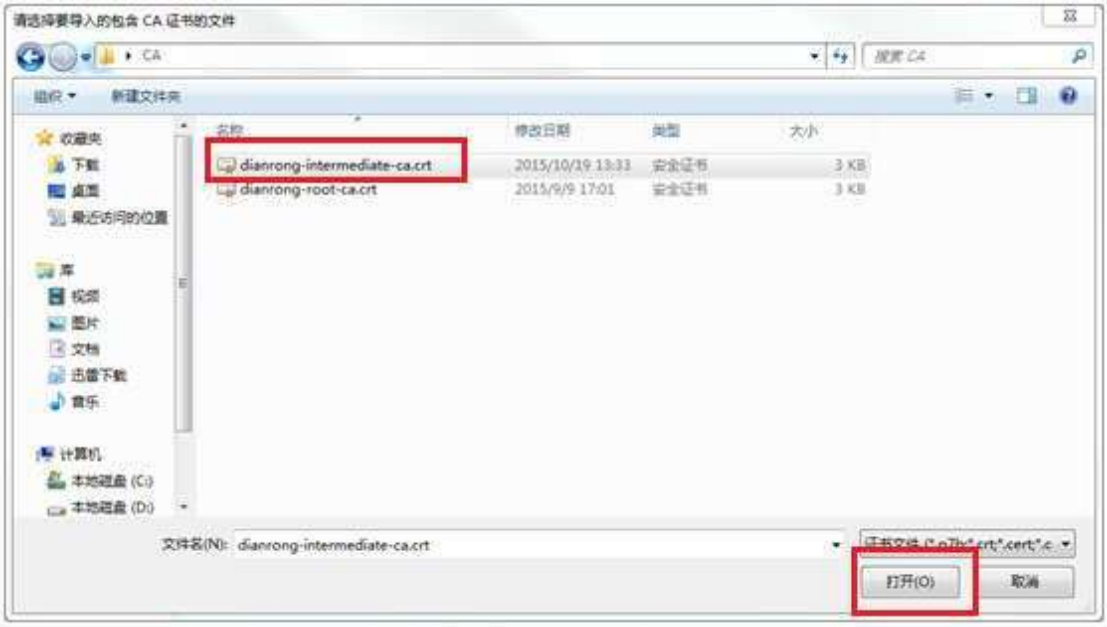


6．核对 sha1 指纹

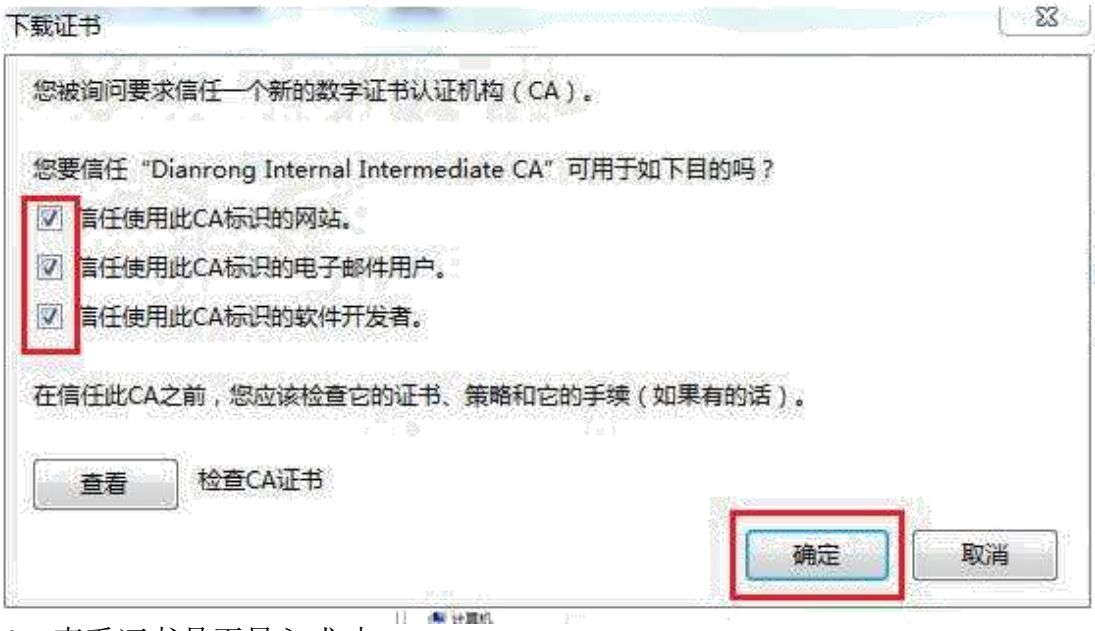


7．再次选择证书机构项，点击导入

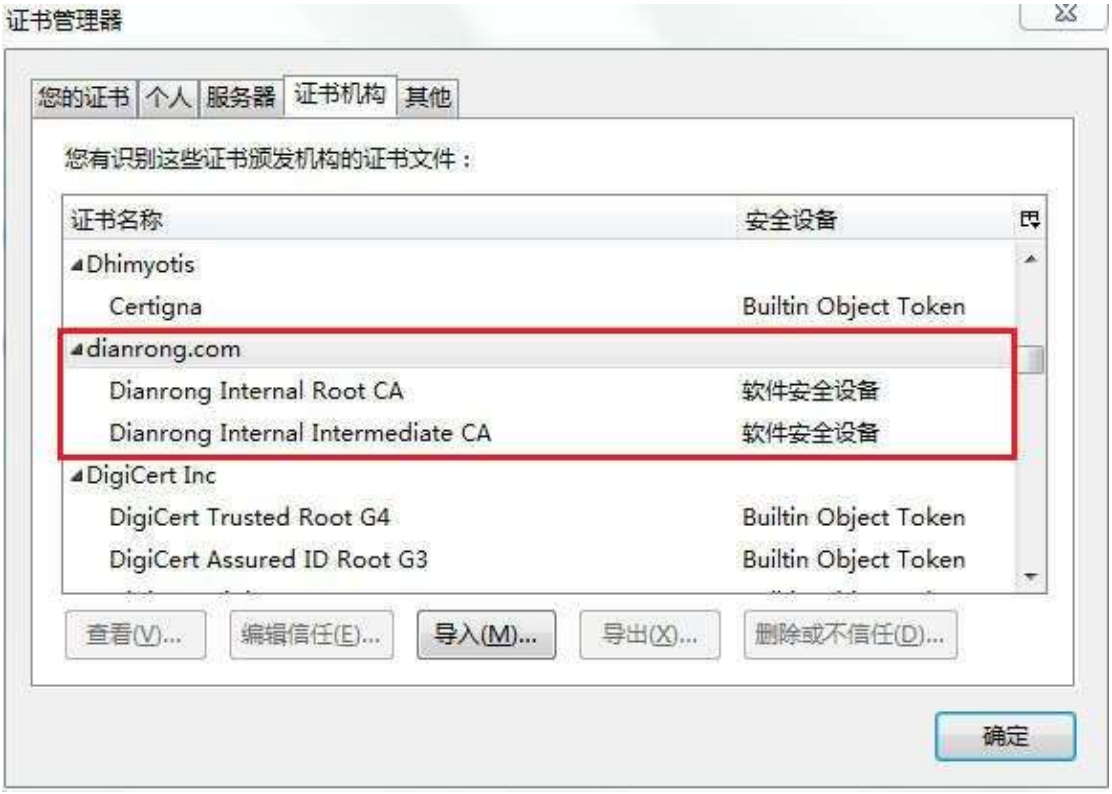
8．选择二级证书，点击打开



9．对该证书配置信任，建议全部勾选，点击确定

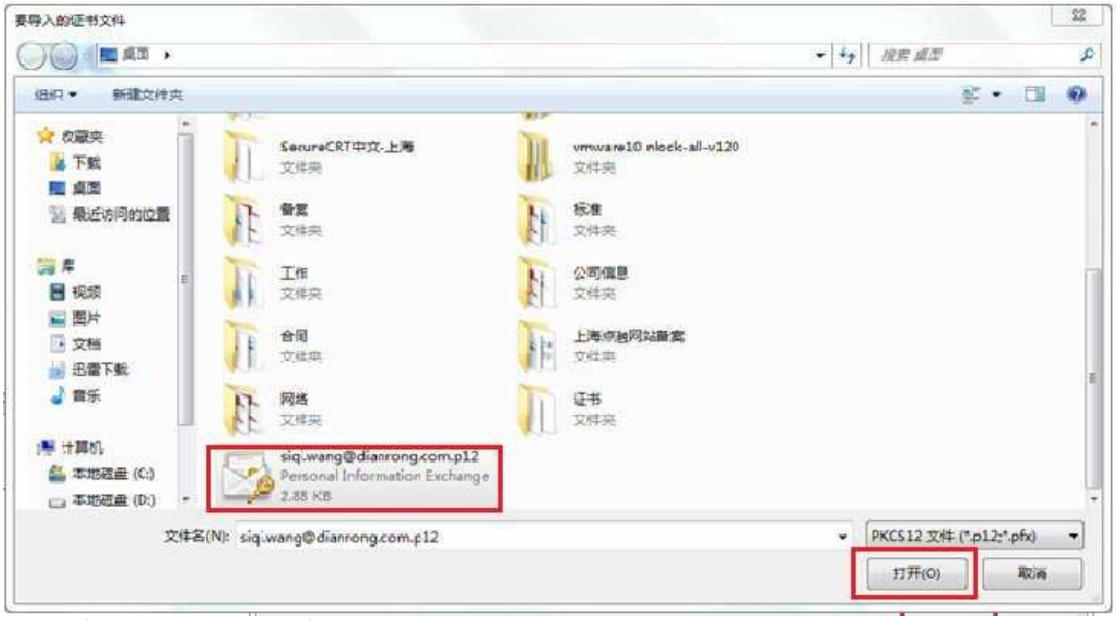


10．查看证书是否导入成功



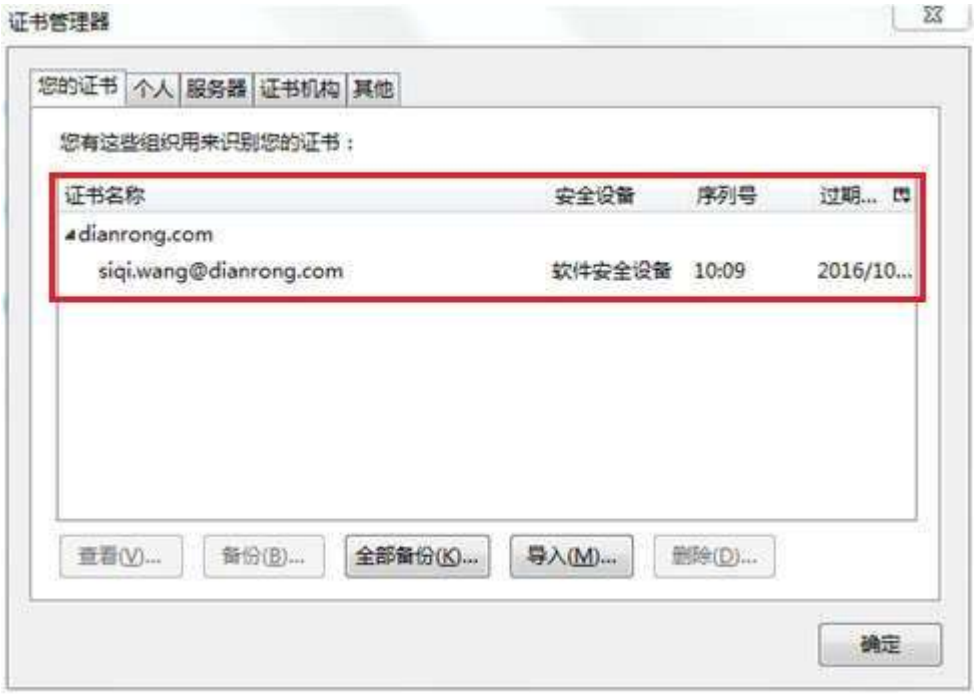
11．选择您的证书，点击导入

12．选择个人证书，点击打开



13．输入密码，点击确定

14. 查看证书导入是否成功



15. 再次连接应用，是否通过同样提供一个公司内部测试 URL：https://testcer.corp.dianrong.com/

如果可以访问不报 400SSL 错误就说明证书安装成功