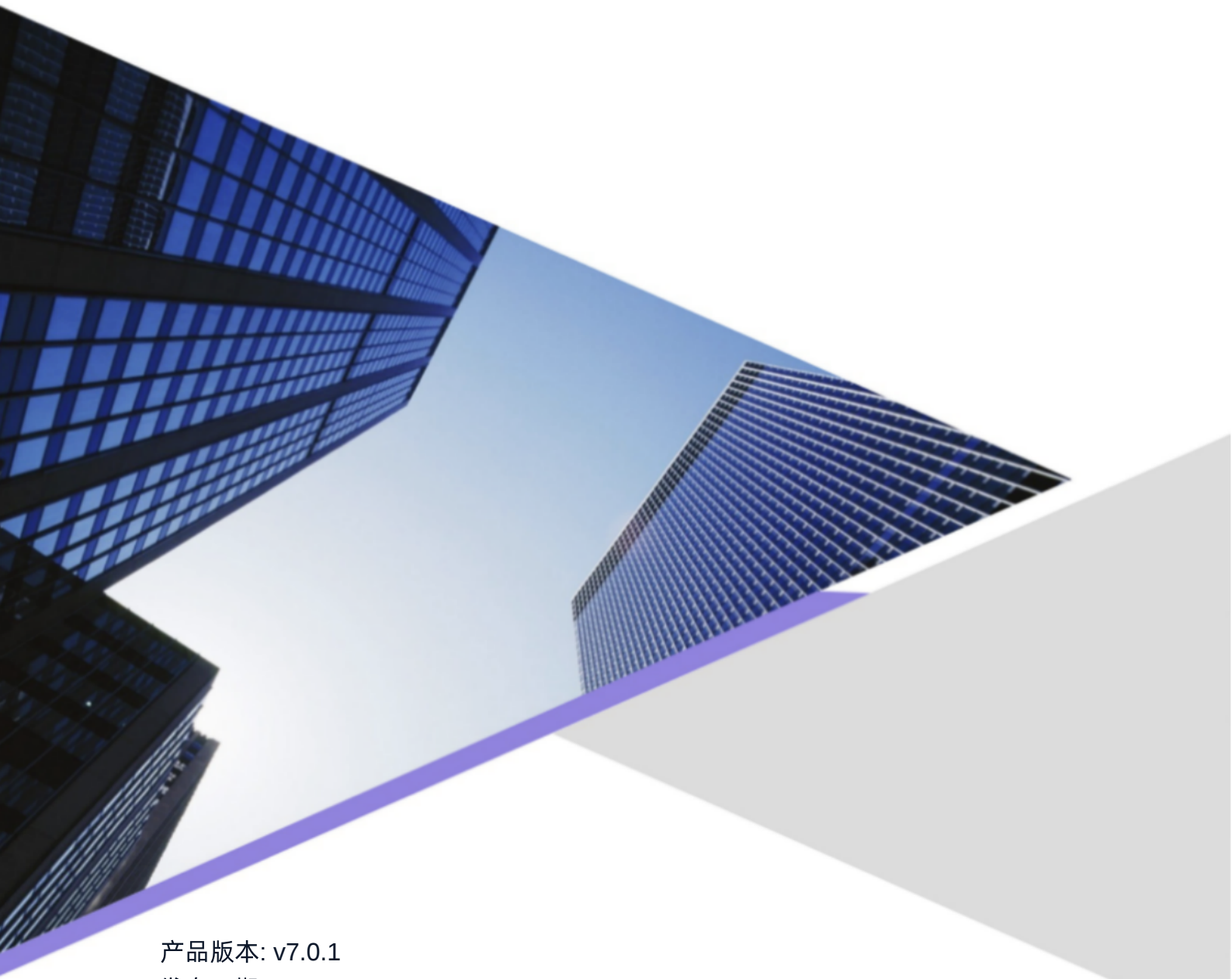
EasyStack
易捷行云

证书与密钥服务

常见问题



产品版本: v7.0.1
发布日期: 2026-08-20

目录

1 常见问题

1.1 客户端如何导入私有CA证书到受信任的证书颁发机构中

问题描述

客户端访问服务时，浏览器提示 “您的连接不是私密连接“等安全告警信息，错误代码示例为 **NET::ERR_CERT_AUTHORITY_INVALID**，如下图所示：

问题原因

本产品提供的是私有CA服务，不在浏览器及操作系统默认的受信任颁发机构中。使用本产品生成的私有证书配置了HTTPS的服务后，仍需在客户端安装证书链到受信任的证书颁发机构中。

解决方案

请参考本章节内容，将私有CA添加到受信任的证书办法机构中。

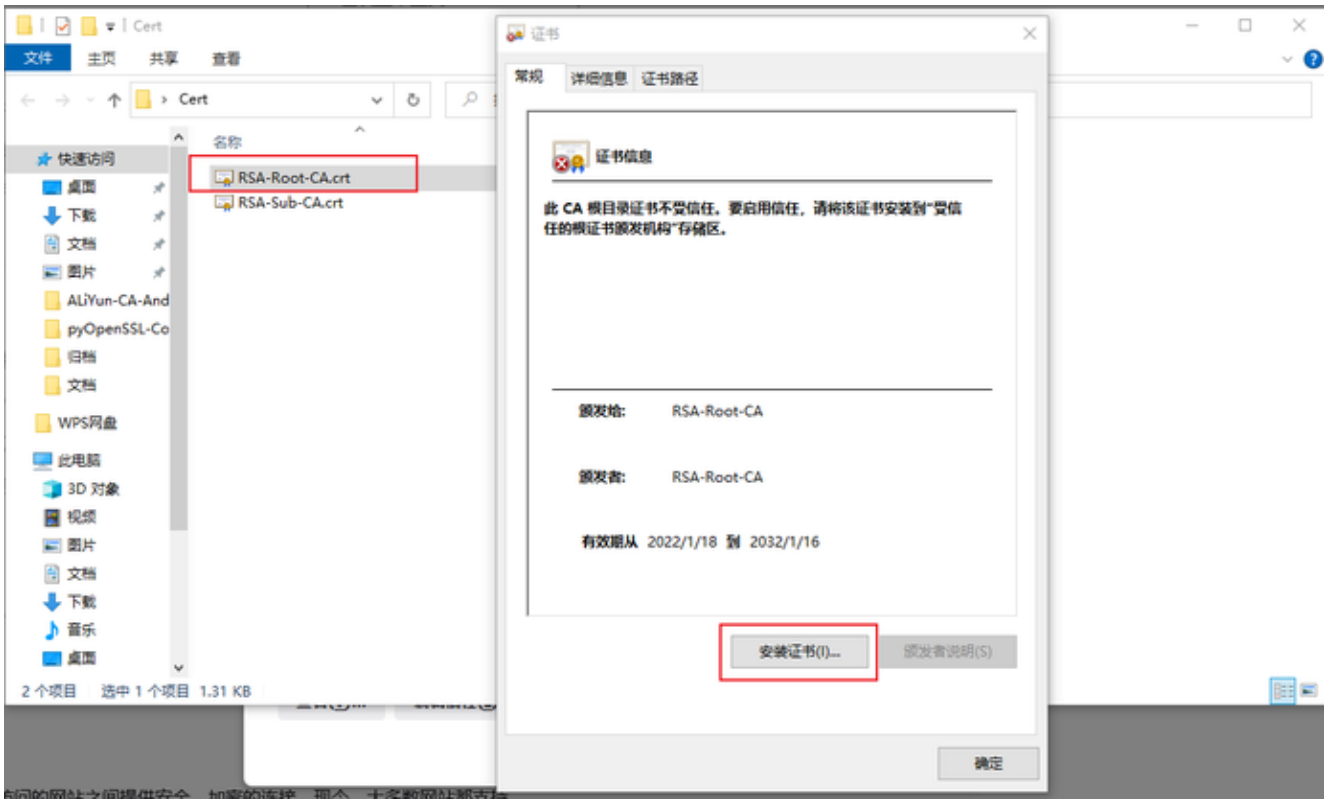
> 说明：
> Firefox浏览器是从浏览器内部的证书库检查当前证书的签发CA是否受浏览器信任，而不是读取操作系统中的证书库，因此其配置方式不同于其它浏览器。

Windows操作系统

本节介绍在Windows操作系统中，如何导入私有证书的签发CA证书链，使其成为受信任的证书颁发机构。

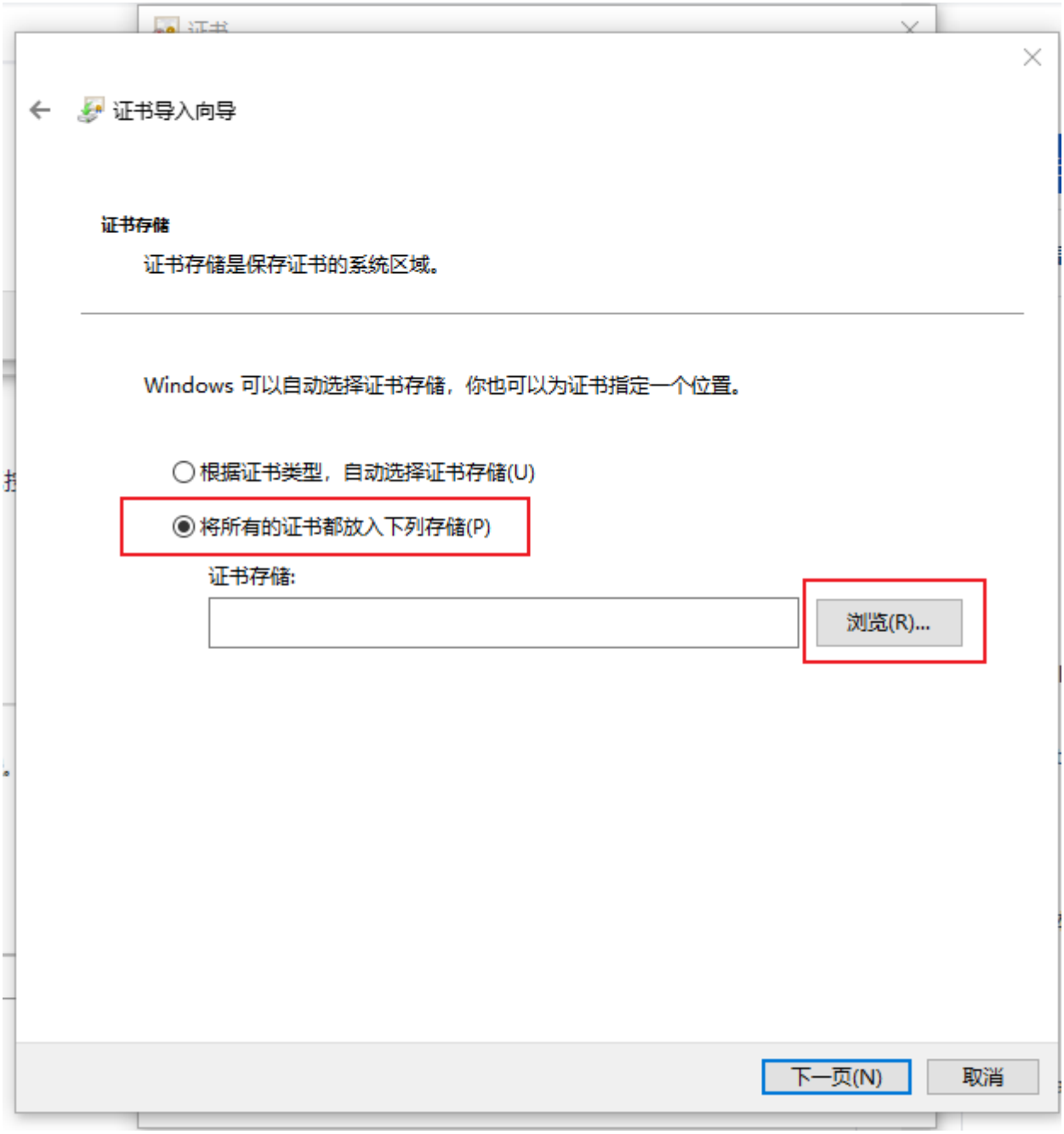
1. 在证书与密钥服务页面，下载该私有证书的签发CA链上所有的CA证书文件，即该证书的签发CA、签发CA的上一级签发CA，以此类推直至根CA。

2. 双击某个CA证书文件，在弹出的窗口中单击 `安装证书` 。

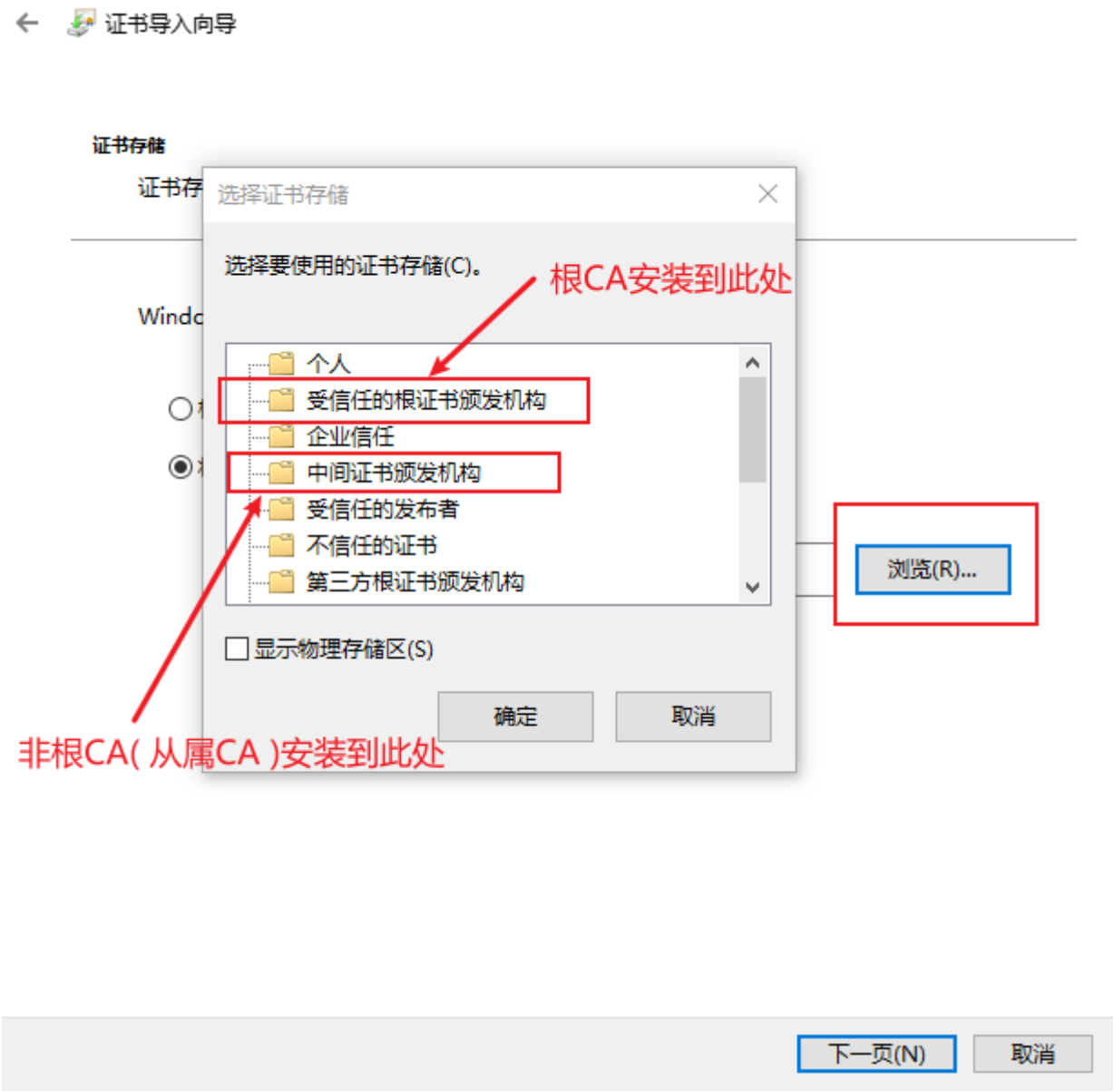


3. 存储位置选择 `当前用户` ，单击 `下一页` 。

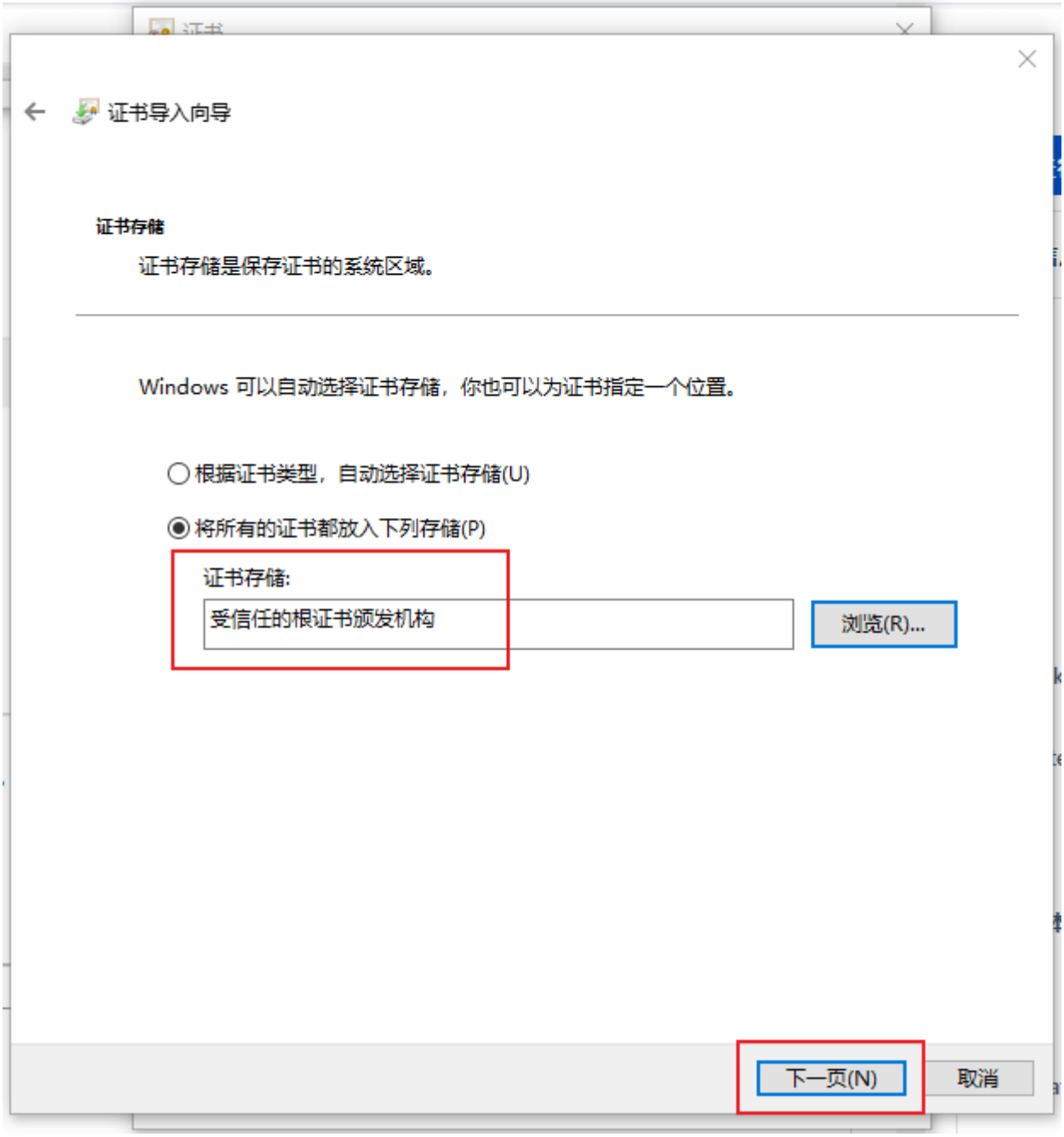
4. 选择 `将所有的证书都放入下列存储(P)` 。



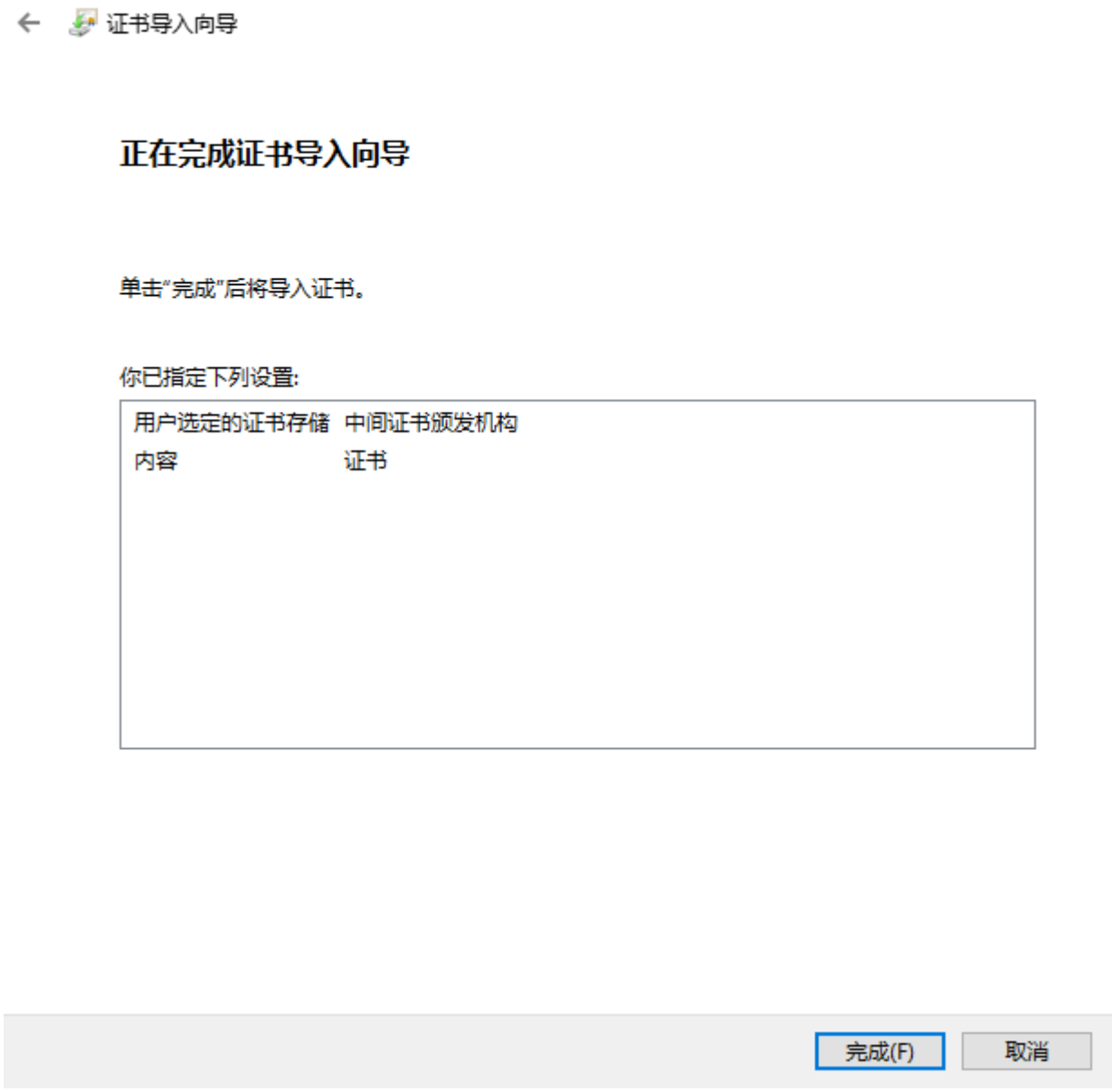
5. 单击 `浏览` ，如果是根CA选择 `受信任的根证书颁发机构` ，如果是从属CA选择 `中间证书颁发机构` 。选择完成后单击 `确定` 。


证书导入向导
证书存储
证书存
选择证书存储
选择要使用的证书存储(C)。
根CA安装到此处
个人
受信任的根证书颁发机构
企业信任
中间证书颁发机构
受信任的发布者
不信任的证书
第三方根证书颁发机构
浏览(R)...
显示物理存储区(S)
确定
取消
非根CA(从属CA)安装到此处
下一页(N)
取消

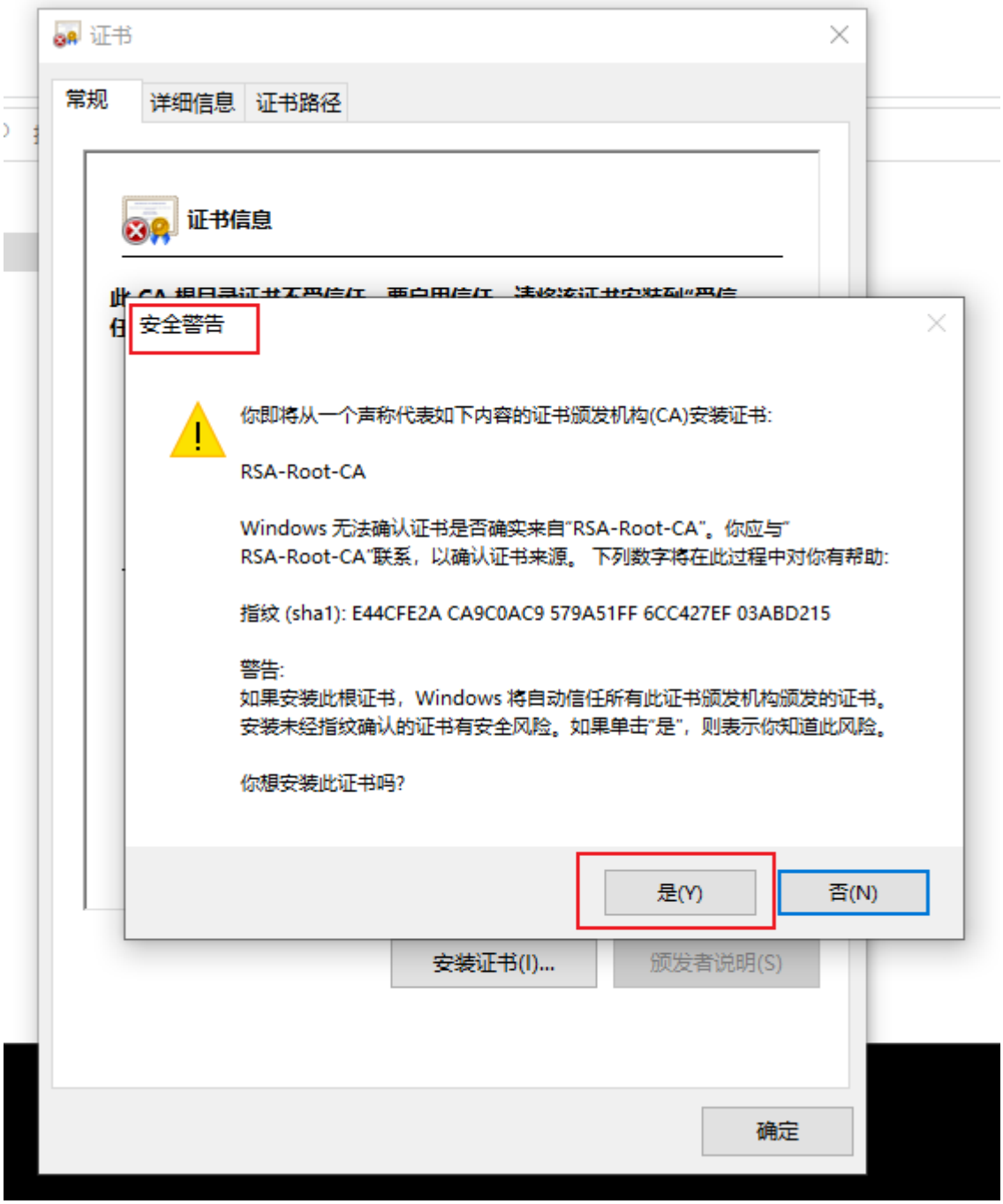
6. 单击 `下一页` 。

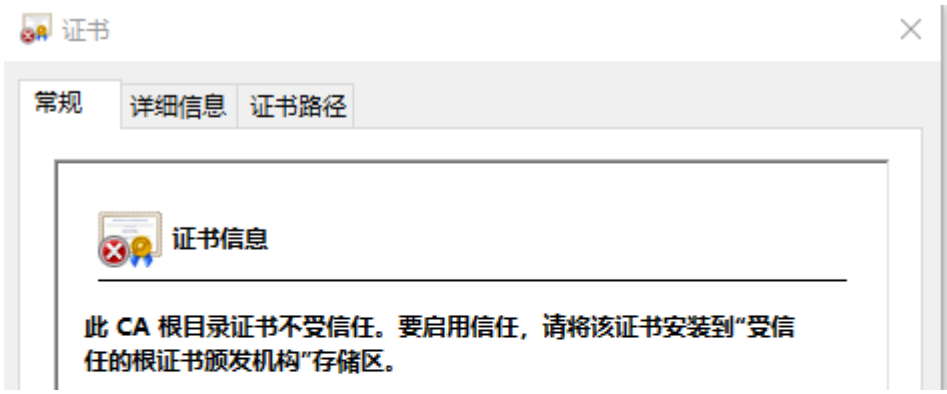


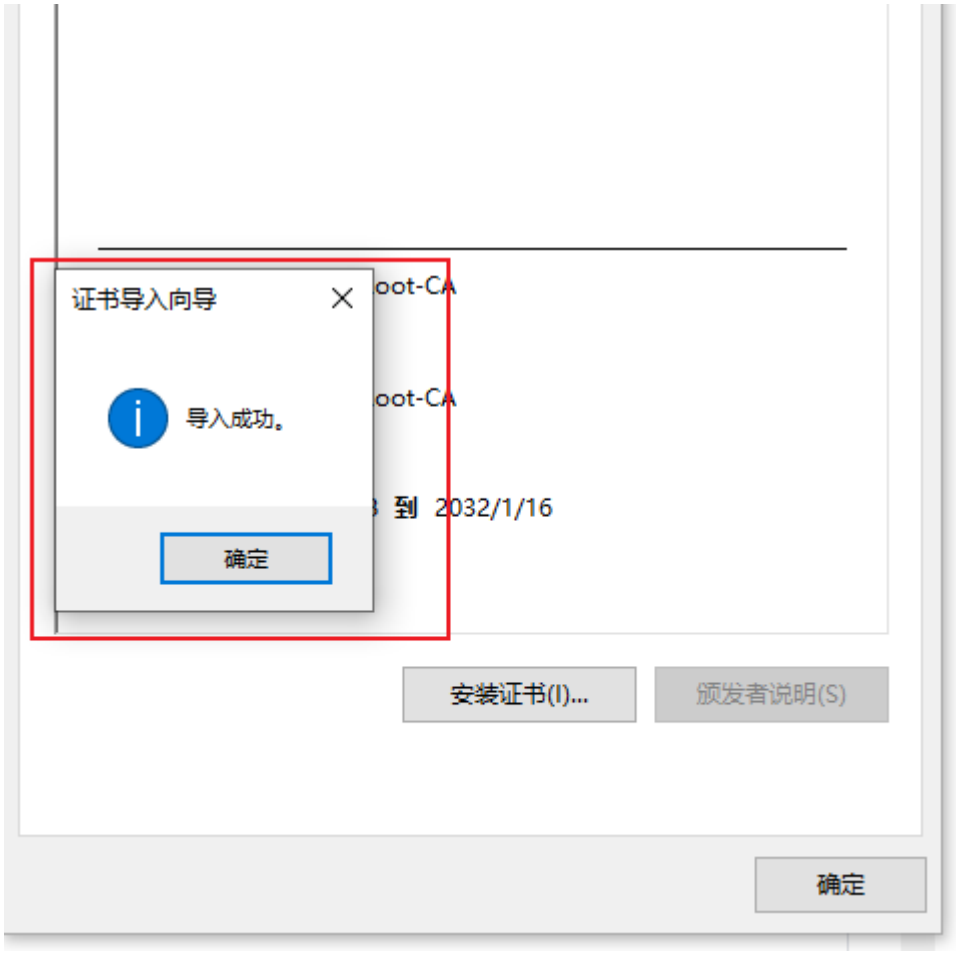
7. 单击 `完成` ，弹出安全警告窗口。


证书导入向导
正在完成证书导入向导
单击"完成"后将导入证书。
你已指定下列设置:
用户选定的证书存储 中间证书颁发机构
内容 证书
完成(F)
取消

8. 单击 `是` ，提示导入成功。


证书
常规
详细信息
证书路径
证书信息
安全警告
你即将从一个声称代表如下内容的证书颁发机构(CA)安装证书:
RSA-Root-CA
Windows 无法确认证书是否确实来自"RSA-Root-CA"。你应与"RSA-Root-CA"联系，以确认证书来源。 下列数字将在此过程中对你有帮助:
指纹 (sha1): E44CFE2A CA9C0AC9 579A51FF 6CC427EF 03ABD215
警告:
如果安装此根证书，Windows 将自动信任所有此证书颁发机构颁发的证书。安装未经指纹确认的证书有安全风险。如果单击"是"，则表示你知道此风险。
你想安装此证书吗?
是(Y)
否(N)
安装证书(I)...
颁发者说明(S)
确定


证书
常规
详细信息
证书路径
证书信息
此 CA 根目录证书不受信任。要启用信任，请将该证书安装到"受信任的根证书颁发机构"存储区。



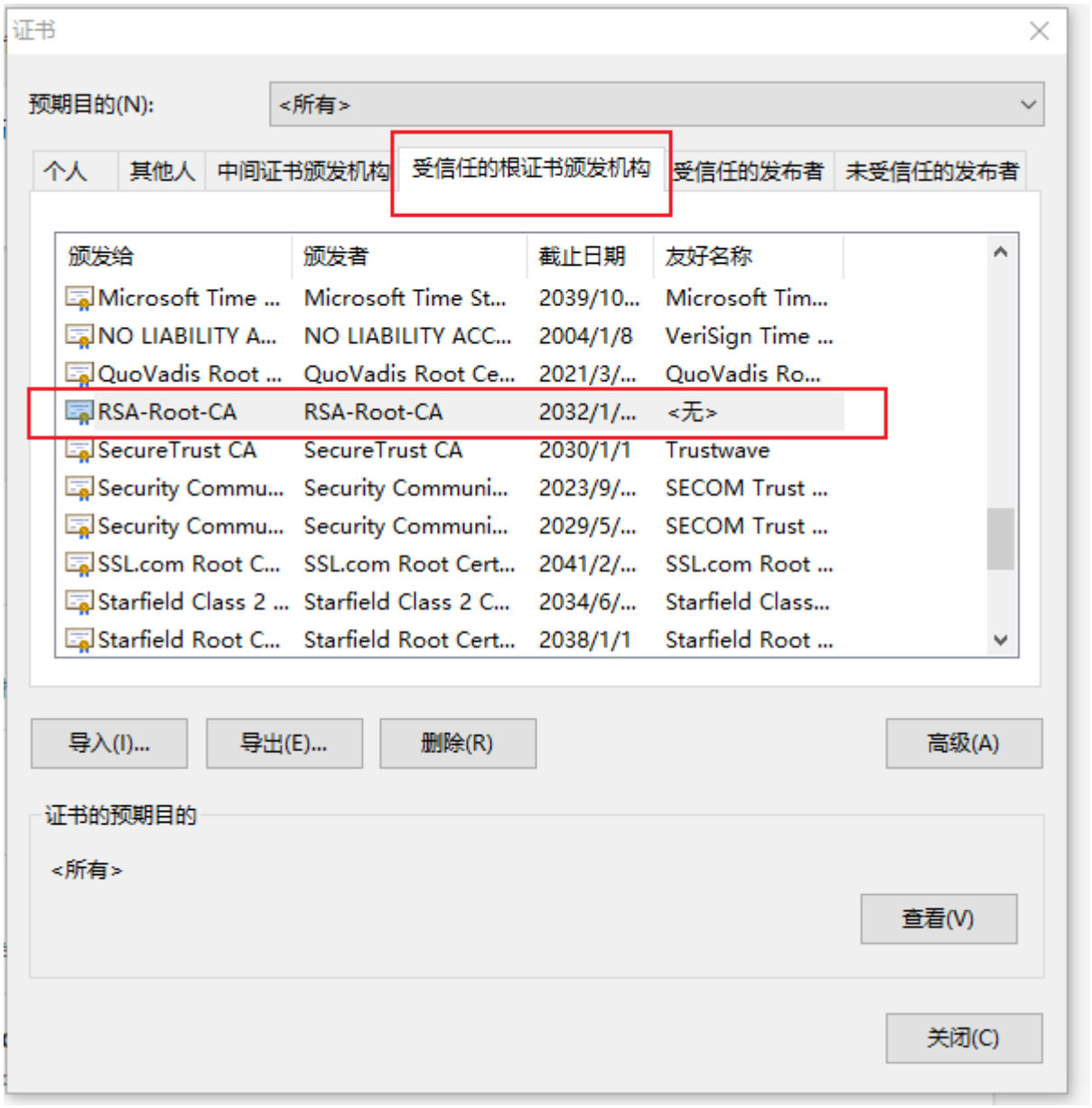
9. 重复以上步骤，依次安装该私有证书的签发CA到根CA的所有CA证书。

10. 在浏览器中验证证书导入结果，以Microsoft Edge浏览器为例。

    1. 打开Microsoft Edge浏览器，进入设置页面。

2. 在 “隐私、搜索和服务” 菜单项中找到 “安全性”，单击“管理证书”。

3. 在弹出的证书窗口中，查看“受信任的根证书颁发机构” 和“中间证书颁发机构”页签，即可查看到导入的根CA证书和从属CA证书。

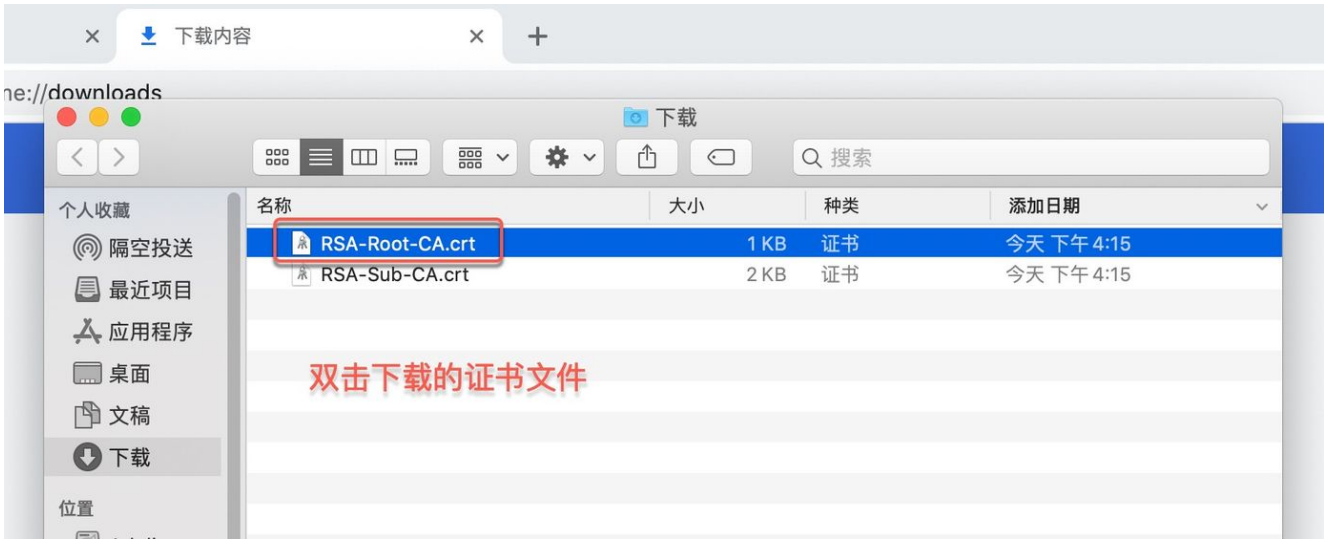


macOS操作系统

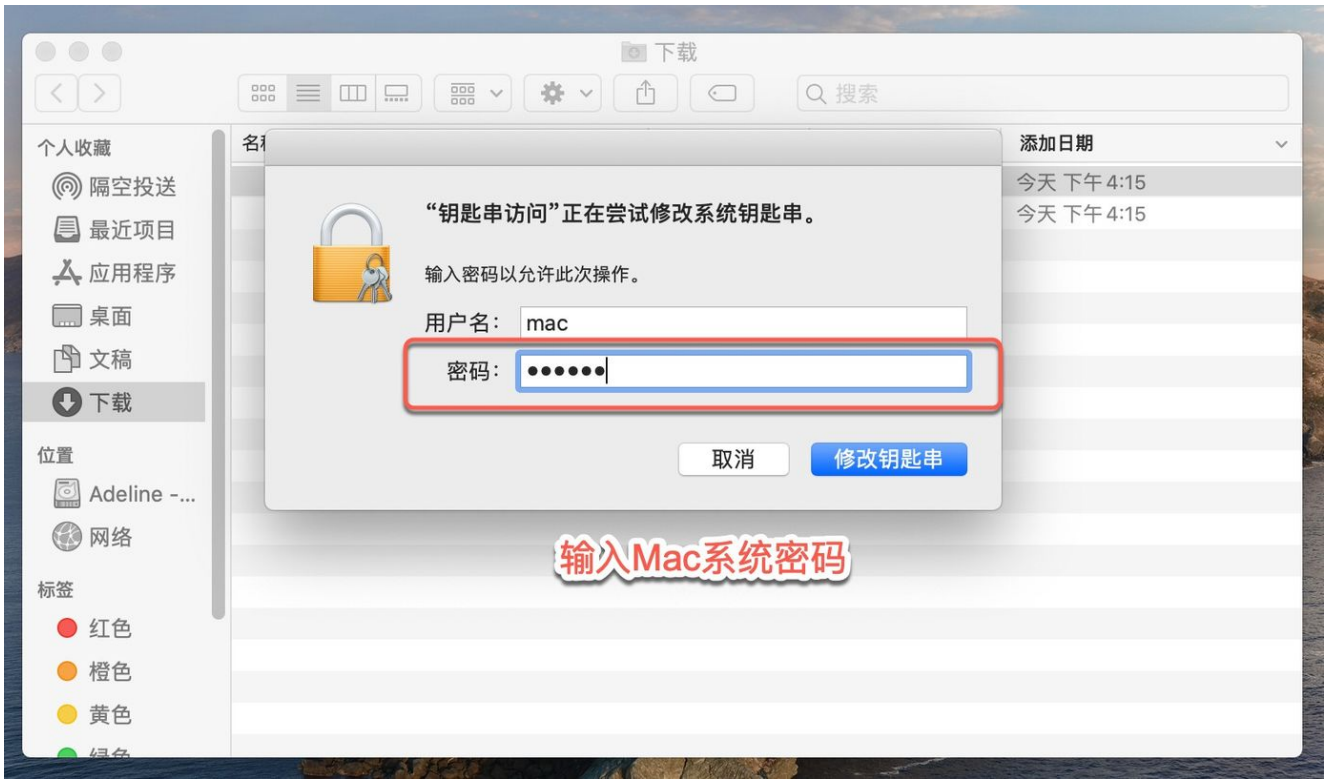
本节介绍在macOS操作系统中，如何导入私有证书的签发CA证书链，使其成为受信任的证书颁发机构。

1. 在证书与密钥服务页面，下载该私有证书的签发CA链上所有的CA证书文件，即该证书的签发CA、签发CA的上一级签发CA，以此类推直至根CA。

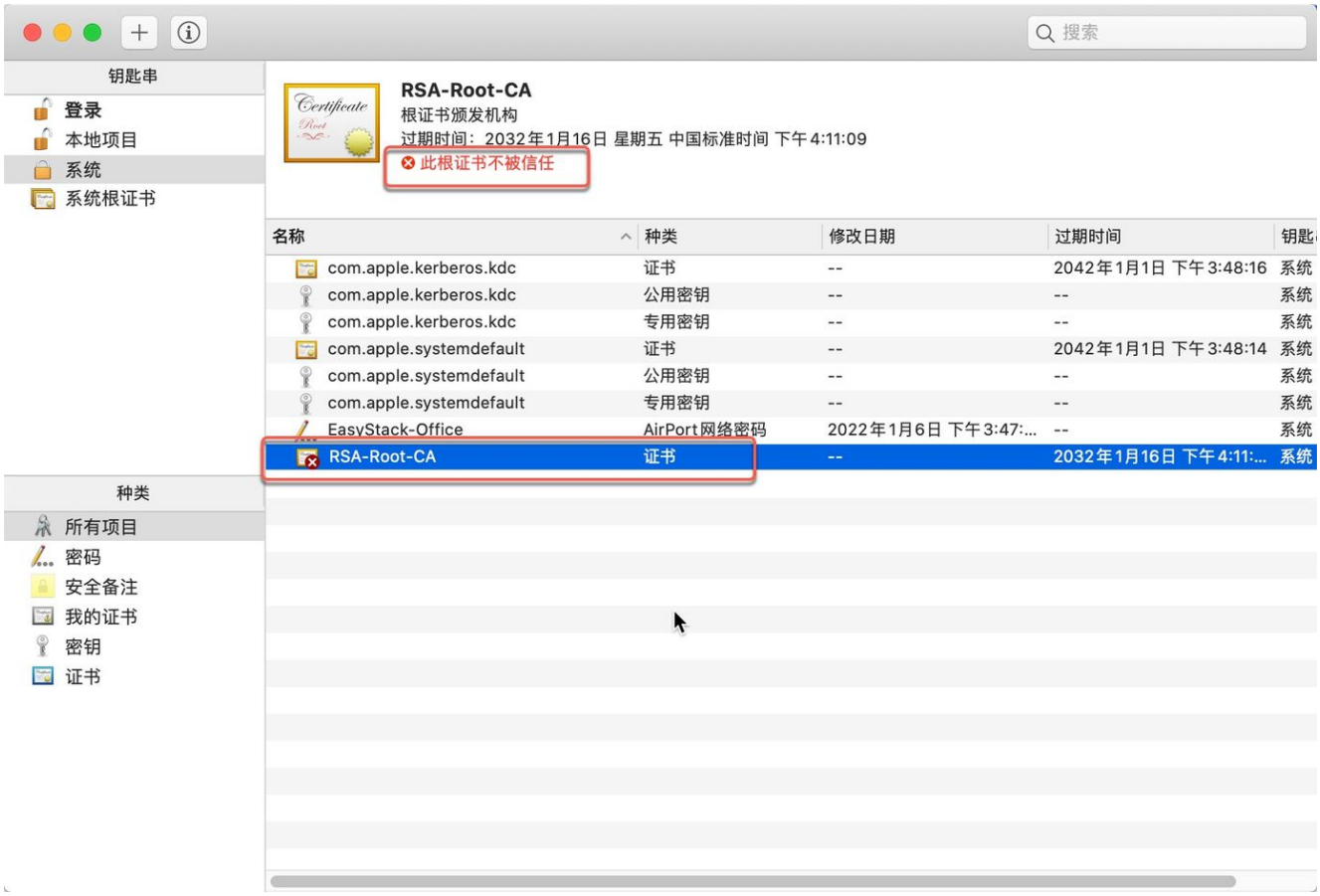
2. 双击某个证书文件，弹出密码输入窗口。



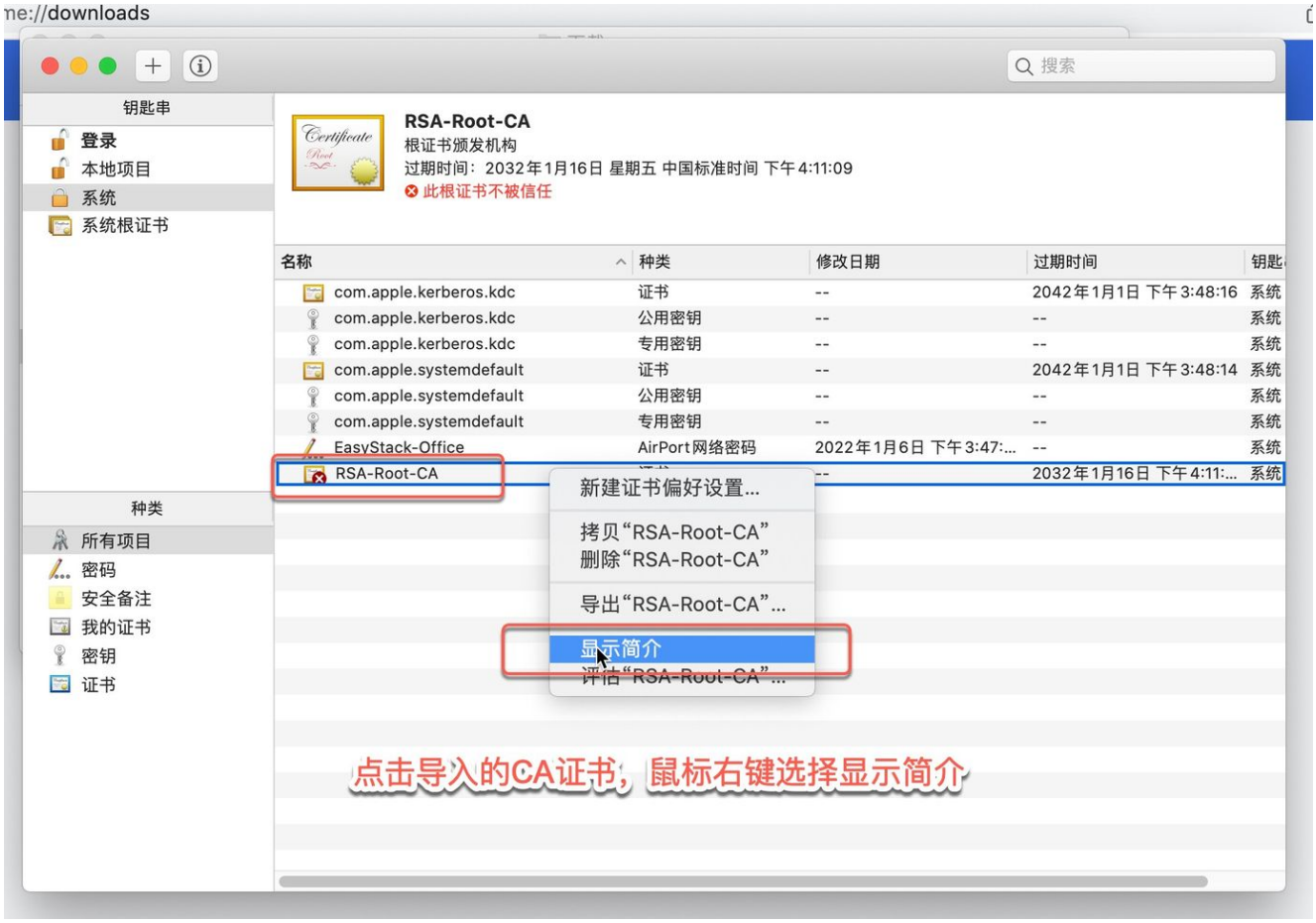
3. 输入系统密码，单击 `修改钥匙串` ，弹出钥匙串列表。



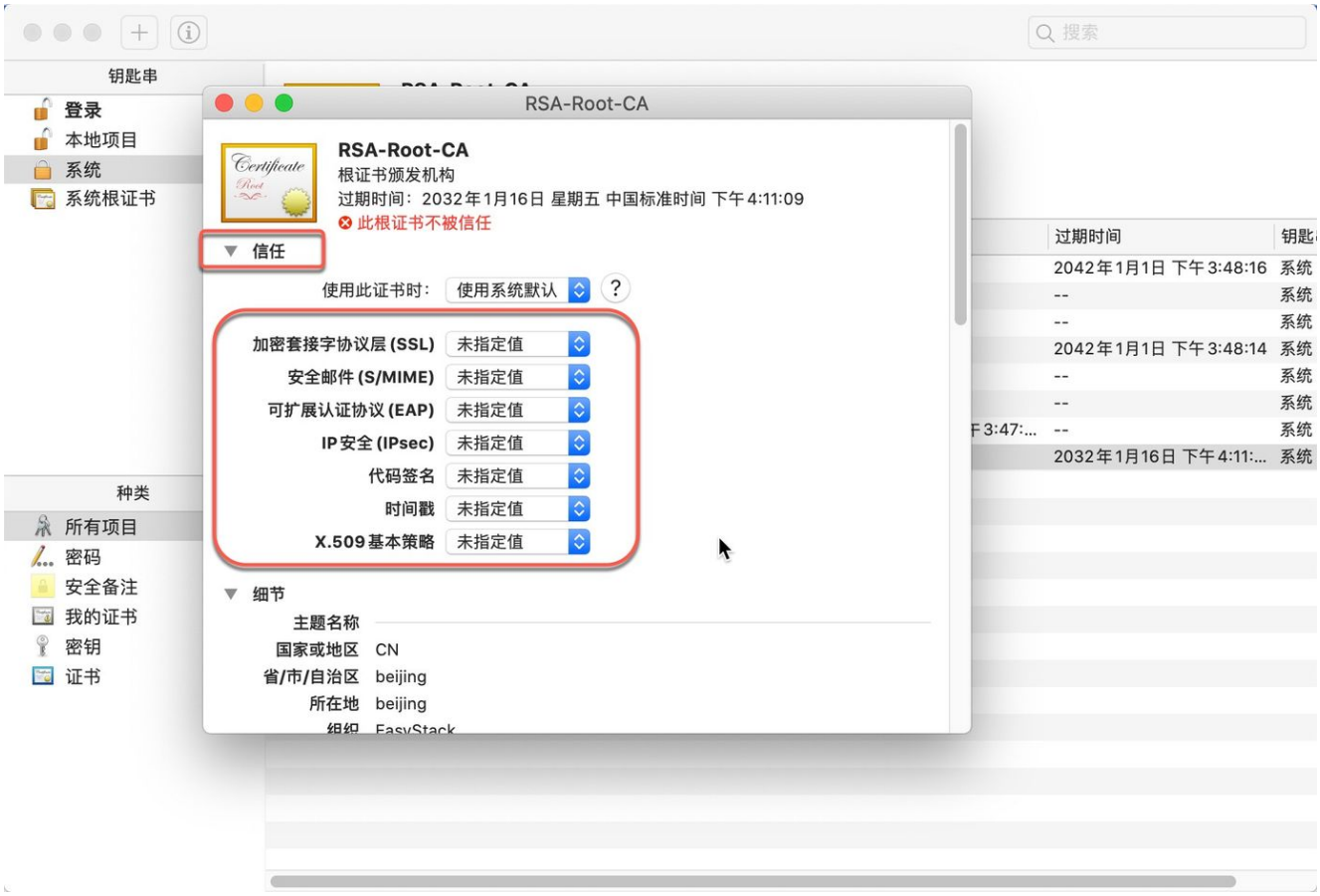
4. 此时虽然私有CA的证书已经导入到系统钥匙串中，但仍不受系统信任。



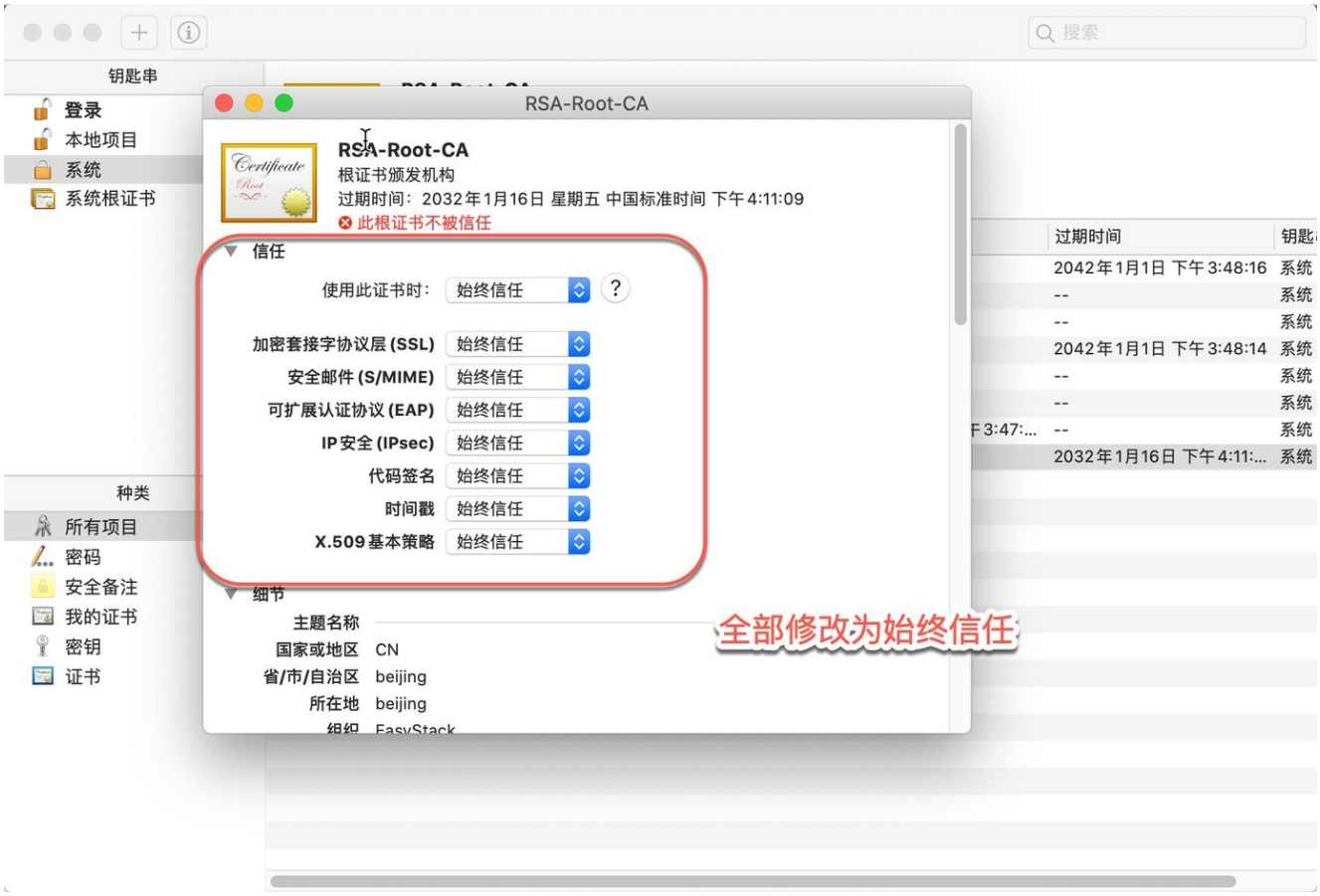
5. 右键单击导入的私有CA证书，选择“显示简介”。



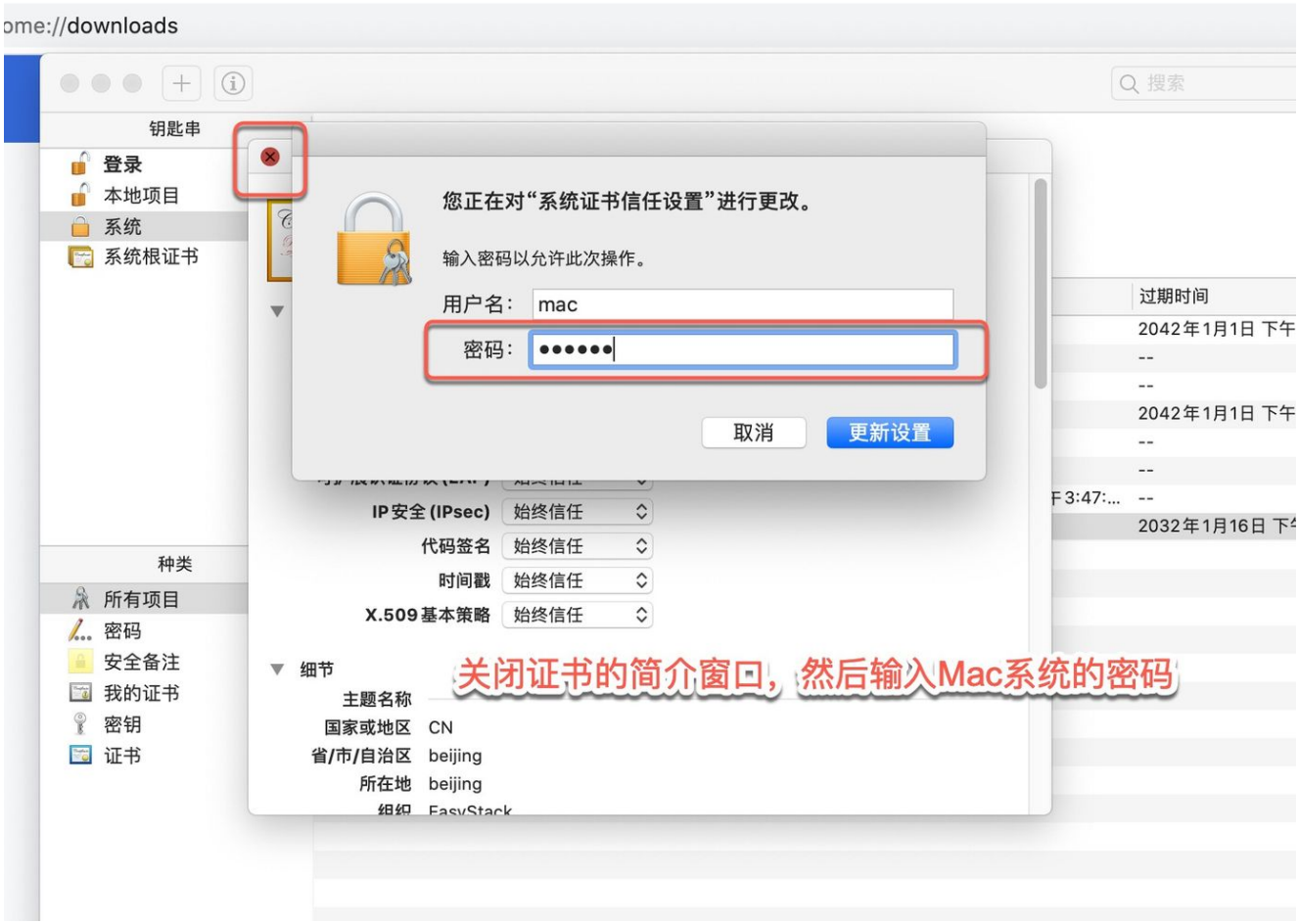
6. 展开“信任”下的详细信息。



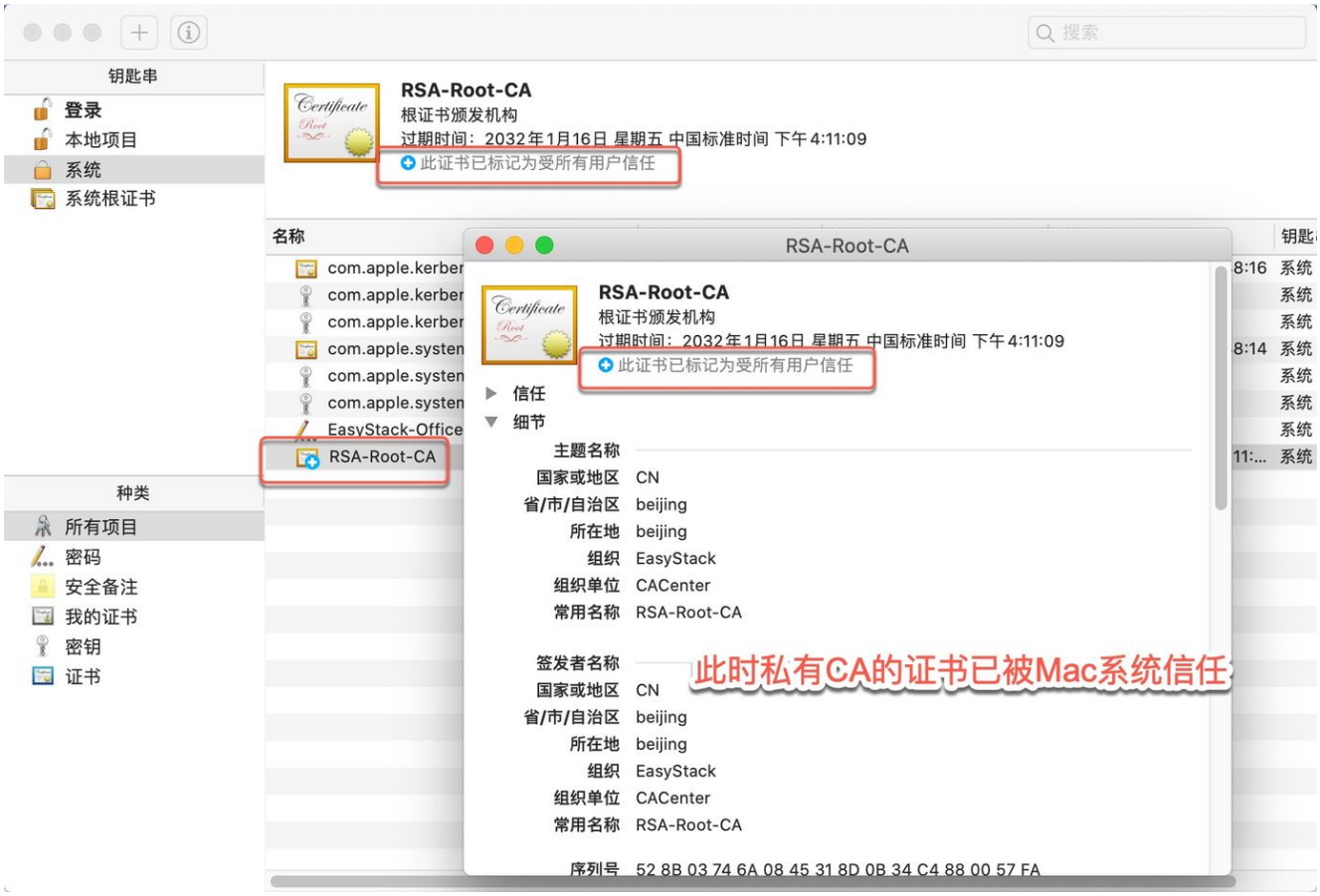
7. 将详细信息中的所有选项改为“始终信任”。



8. 关闭窗口。此时由于修改了文件属性，需要再次输入系统密码。



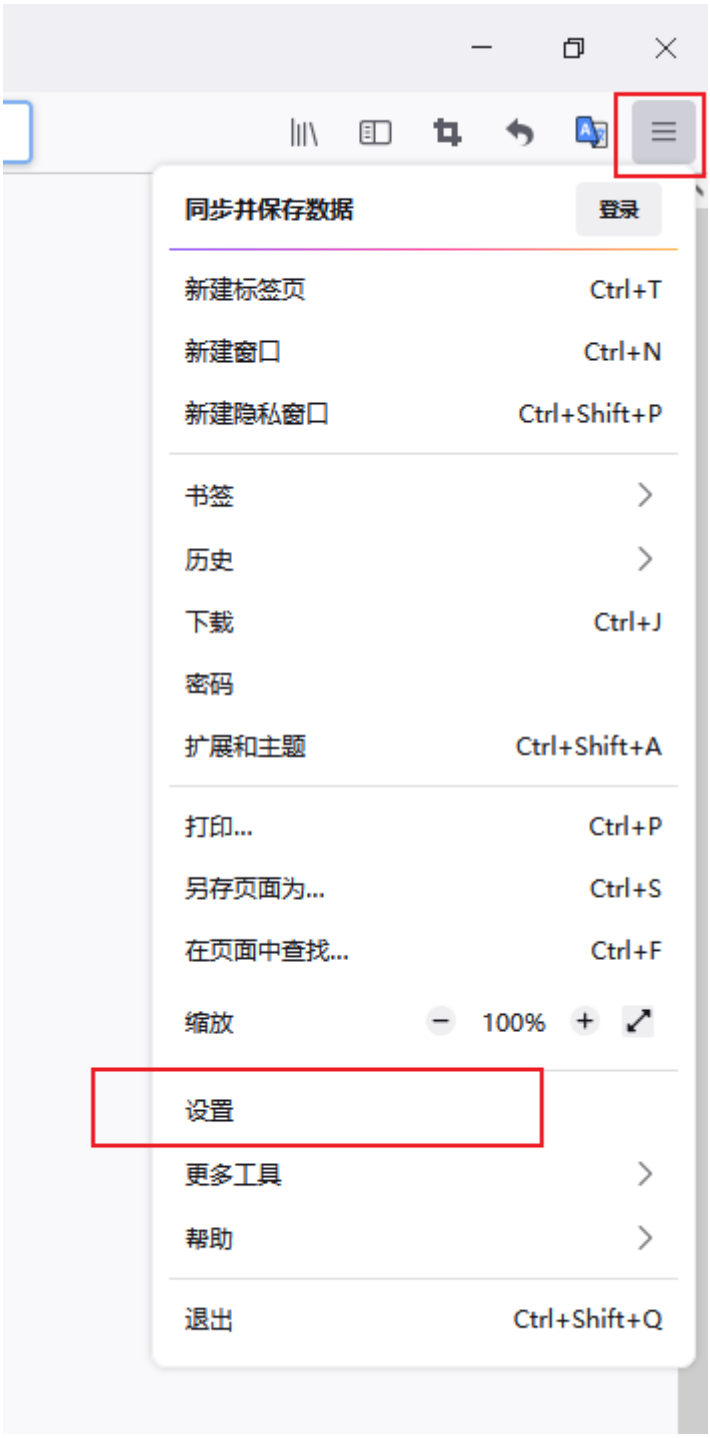
9. 再次在钥匙串列表中查看导入的私有CA证书，已被系统信任。



Firefox浏览器

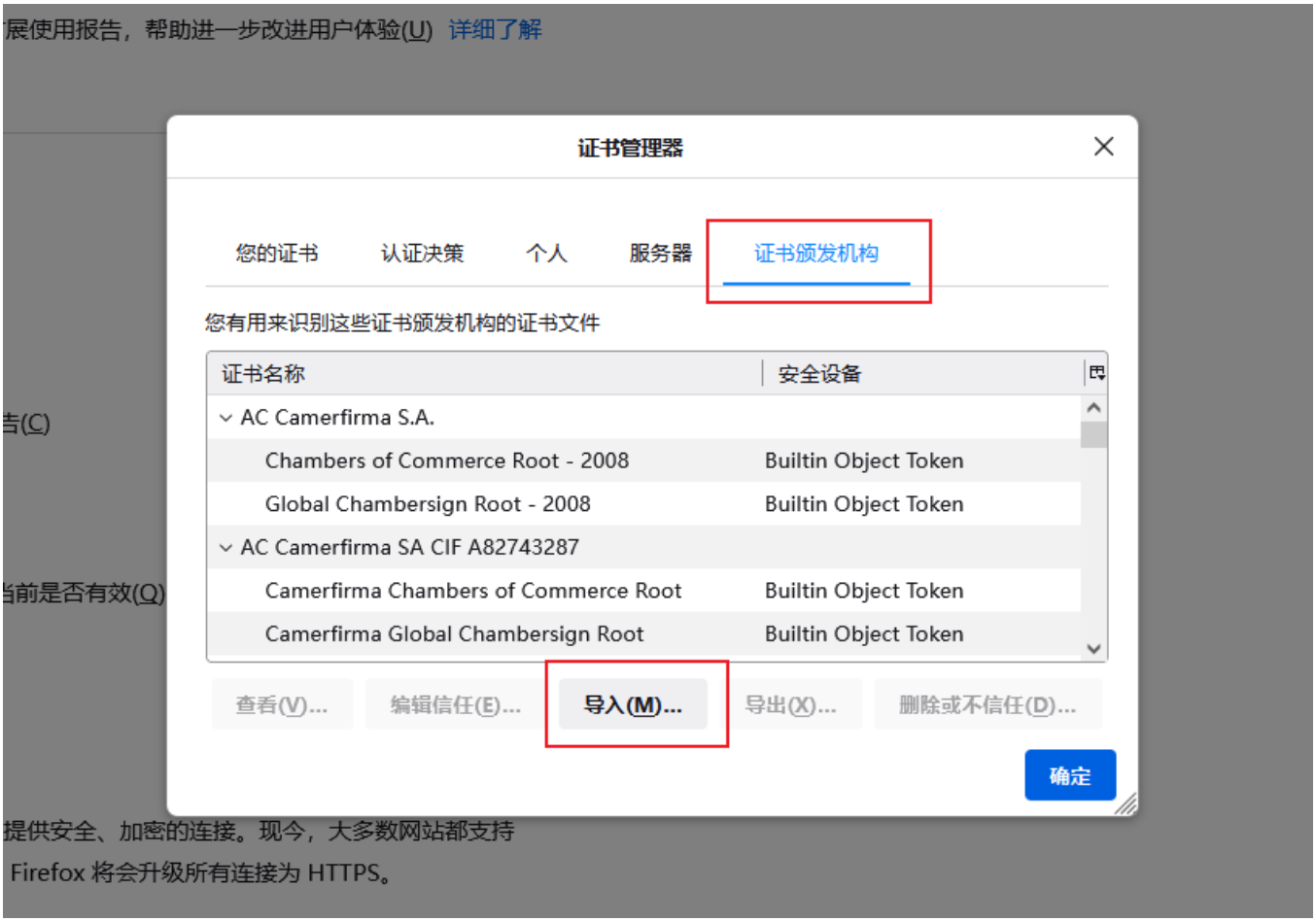
本节介绍如何在Firefox浏览器中导入私有证书的签发CA证书链，使其成为受信任的证书颁发机构。

1. 在证书与密钥服务页面，下载该私有证书的签发CA链上所有的CA证书文件，即该证书的签发CA、签发CA的上一级签发CA，以此类推直至根CA。
2. 打开 Firefox 浏览器设置页面。

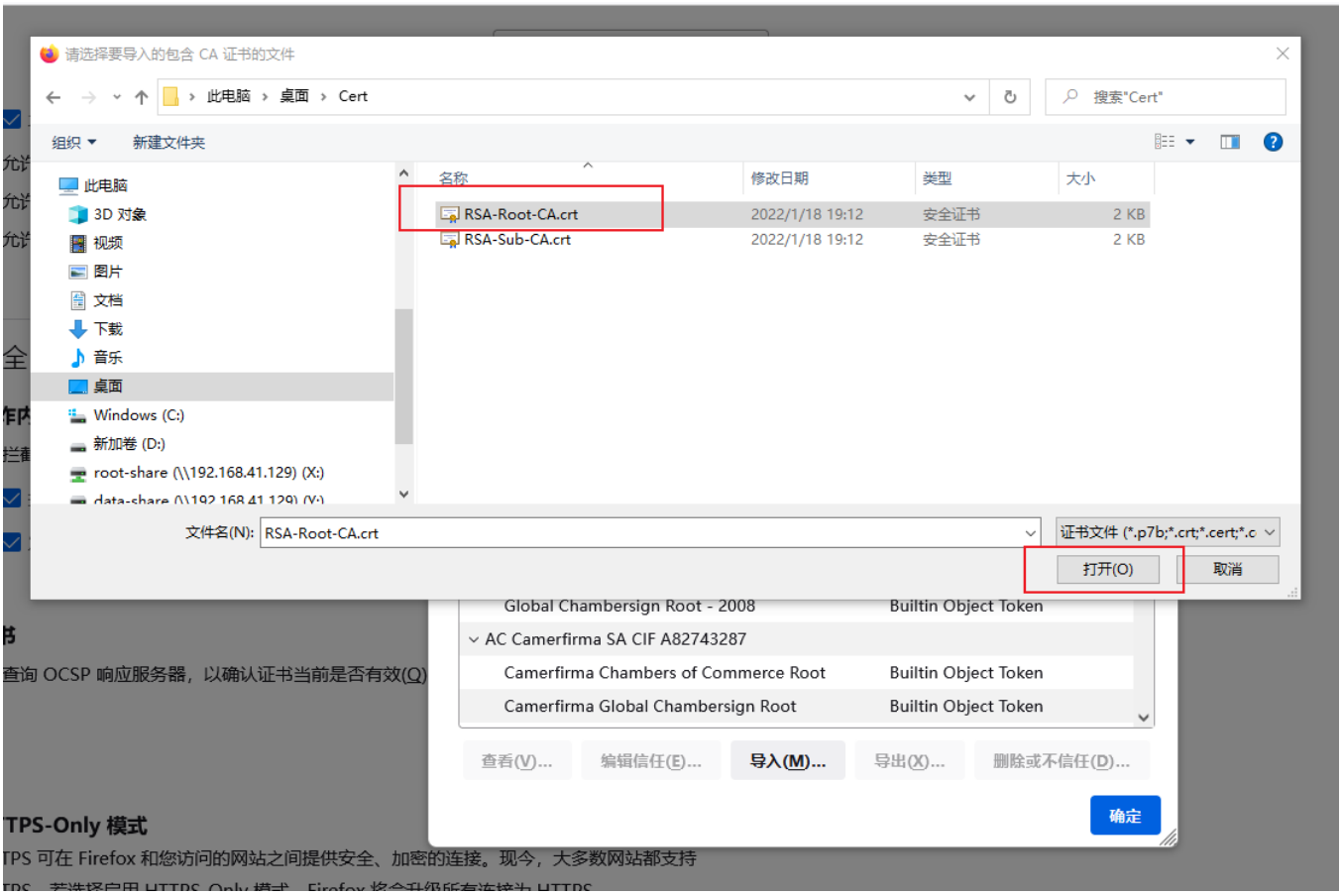


3. 在“隐私与安全”菜单项中，找到“证书”，单击 查看证书 。

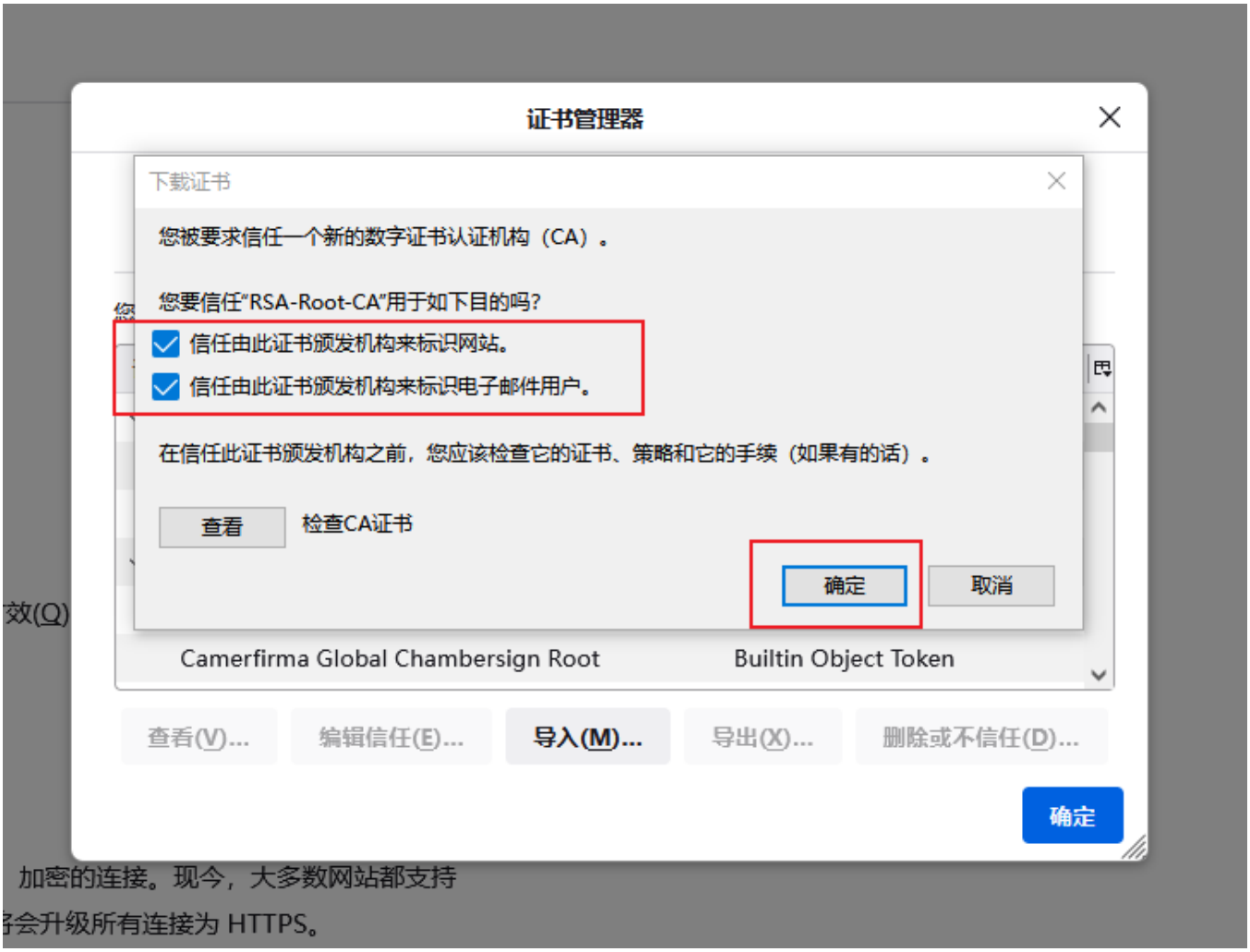
4. 在弹出的证书管理器中，选择“证书颁发机构”页签，单击 `导入` 。



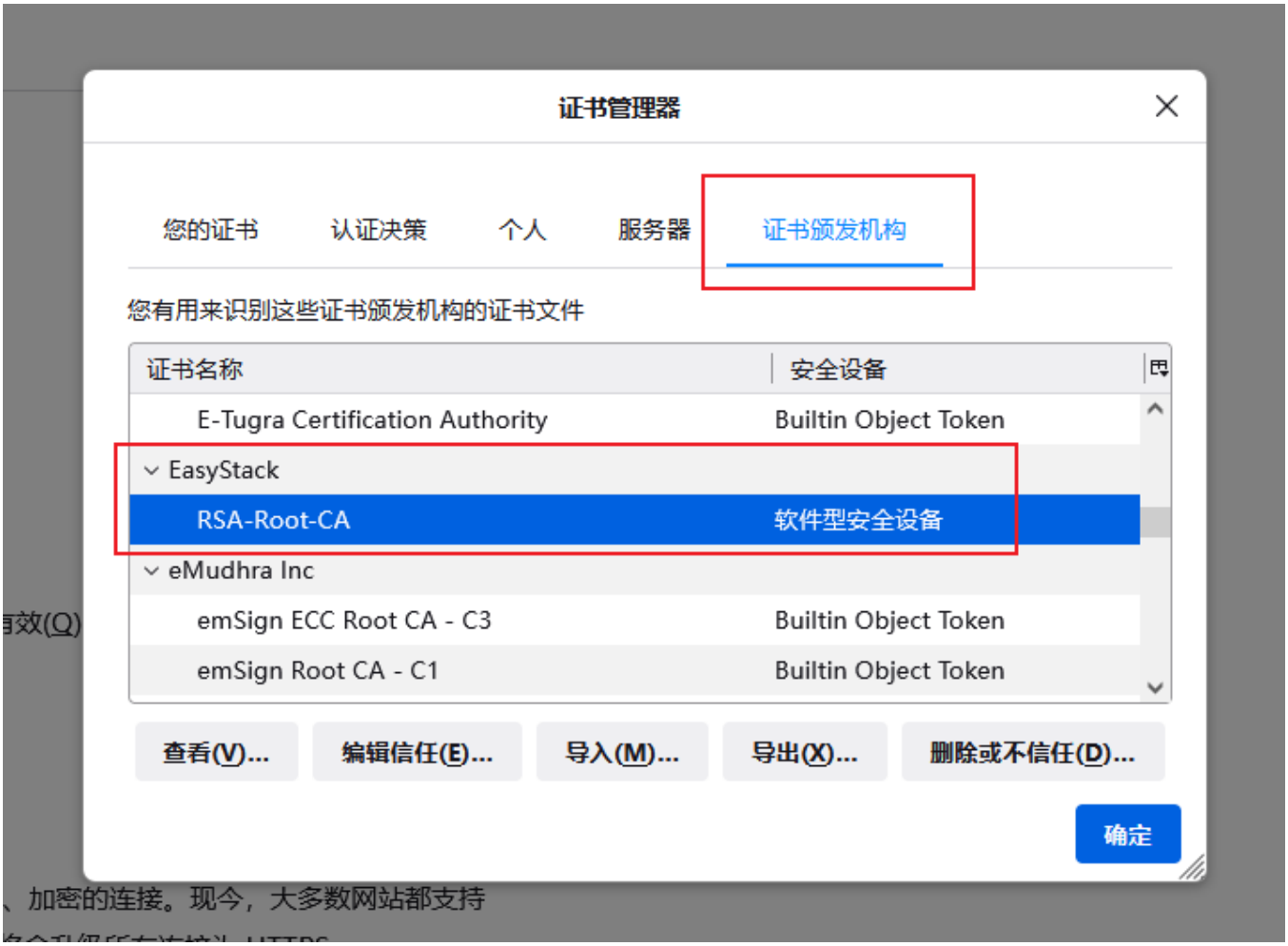
5. 选择下载好的私有CA证书文件，单击 `打开` 。



6. 勾选 “信任由此证书颁发机构来标识网站” 和 “信任由此证书颁发机构来标识电子邮件用户”选项，单击 `确定` 。



7. 私有证书导入成功，可在"证书管理器"窗口中的"证书颁发机构"页签下看到已导入的私有CA。



8. 重复以上步骤，安装该私有证书的签发CA到根CA的所有CA证书。

1.2 服务端证书未指定域名，访问服务时提示安全风险

问题描述

客户端访问服务时，浏览器提示 “您的连接不是私密连接” 或者 “警告：面临潜在的安全风险“ 等安全告警信息，Google浏览器中错误代码显示为 **NET::ERR_CERT_COMMON_NAME_INVALID**，Firefox浏览器中错误代码显示为 **SSL_ERROR_BAD_CERT_DOMAIN**，如下图所示：

问题原因

在访问 HTTPS 服务时，浏览器会检查当前访问的域名与HTTPS服务配置的证书主体的公用名是否一致，如果不一致，浏览器会认为存在安全隐患，则会给出安全风险提示信息。而不一致的根本原因可能为以下两种情况：

- 创建服务端证书时，在“公用名(CN) ”参数处未配置域名；
- 客户端访问的域名与创建服务端证书时在“公用名(CN) ”参数处配置的域名不同。

解决方案

可通过以下两种方式继续访问该HTTPS服务：

- 方式一：在浏览器出现安全风险提示信息后，点击 `高级` - `继续访问服务` 。
- 方式二：在浏览器地址栏中输入与证书主体中公用名相同的域名进行访问。

1.3 当上传证书时提示私钥格式校验失败，如何排查解决

问题描述

证书与密钥服务云产品支持将第三方生成的证书上传至云平台，进行统一存储与管理，有效提高证书运维效率。但是，当所上传证书的私钥格式为通用PEM格式，即以 **-----BEGIN PRIVATE KEY-----** 开头，并以 **-----END PRIVATE KEY-----** 结尾时，将提示私钥格式校验失败。

```
[root@centos import-cert-test]#
[root@centos import-cert-test]# cat privkey.pem
-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQDAQTpVFEU9N3fL
YFkUs8HJGnETxM8s9zAYIHCFNgdgfPL+3d63iz5cQjx2UuAddUxRUv3wDYRX/FCN
x6WWVgUCa8K86hSwFvmiNrxiH0CSKj0ZpNwdnxZFVFQIzciEKusH/nEX9BmGsUUc
rDKUJZct+7c+VE7Hqtt7F/SXTxfj6TlrY/WfVDIleveJS18rmpnTfd272hmtG6sw
mNdGnVmF0G36R7feIaArRqwq2j6iygo7M64jR2eZ6vAuORF5o4yl35EpRO/SvarL
gEJFXXWFrrn0PbsRP+Q0ASEcp1DNUx1C8ah3cXmr0//XGZoY50hKEKDfrRdwB/Z2
qxl/2cDfAgMBAAECggEBAIvw7tzvHFcrAO/w+eav0ebocFbLc2Jvq3pkYoMUiNob
GWWbanp/yKyvKgOW37uRnjO0DVOnAyZoatpI8Kc1hf/1IJMScGyczKje3tEtnnrG
dCMudWq6Wi0s9l5SLBrIgrwW4YtmCw6YCo6MaWSc2CaIiyG7jHyaSZiYH1nkIKer
4L4ry+MbT7UtSZR7jB199fgodx6cP49AEgaLK70Tiq/OfWAX5o5F+jL33mmO+1u8
7w6ynStJRsqNuRODRO7Wrtvyl+WySk6ZByURI0DI9CJqSpquhi1shl9xnpEnt4NG
25G0nBa37NOQLoOjACkpVNBHw6gBCCJqppzy6DudhgECgYEA6pnnz8xRSqIswIe3
ppHmGoMLEETrkuejN7BjPx7p83cgaxffYr468VaEm8Fy5Z3L+jTIIT9/MjDLqqVB
qg8xA6LN/lnJIl2D7QUUH8XP/um/GftEuzdWEpdQsuUMQequg13bD5460DtPTcqG
twp9Kg0LU+dHJubS4w12BtG//78CgYEA0cqBdc+1vdLqnuQDQPHrAGtJ+owqKwIX
dld7hHK/raYkq8i/yoJGi9Y/439xBhq20wsBOz7ZEczI38fsaUAj+6rsM9g620p0
DeUz5JSx+LdVsFh9Lj0oAYuPQVbIedq1m7Hpvt4sCe480TJjYmlV0oqouCvZCbfb
29wgZSjEhuECgYAoNPhlxL6p6+F/ncL76UVmhc7/mtBE/S4b/T8FMmcmMuR7djvy
0GeJtSpFB4KJl+G9oA4spJVIJNTDCk+WtcPQu7ZSQVEXcq+Jj7VDPMPJDIaUDVxa
OcGmrghGoLrZET+XhB5nLtclmQSecHdmJ4YMDvBCEQFAyY6bG1N/F7OwQQKBgQCb
PN0lP0j9qQgCATlDIoBBtCJu6q79WjPgVwXIUVzy8wEpuIfrIxFuwmBOSGxrFvN4
ISmNHIlluYJezUJr85Fs1eKoznVlM8Ai1BrdJwa2w3r93czrnUdwNUQRFlWMjcFa
74DGwwIVaxvHtSCDnuxpuj704UVeApYHD9FM6ajbIQKBgQCCwlA9B1ZgsrR5RHTT
Uqdmq7b4hEsZHTUdckihsrn21zxL69PTNHl8blof0UKZM8iJbiebH9uFKpaiEe0N
fURk3jOBPtL8JZvtJ4Up5b4jY9QWWy8T9QwHfisQQlaTD46TAEgNg4lue7TadDvb
bwPplZjnSrEBxIE1v7lovzJIAA==
-----END PRIVATE KEY-----
[root@centos import-cert-test]#
[root@centos import-cert-test]#
```

问题原因

证书与密钥服务云产品要求所上传证书的私钥格式必须为对应算法格式，如：以 **-----BEGIN RSA PRIVATE KEY-----** 开头，并以 **-----END RSA PRIVATE KEY-----** 结尾的RSA算法私钥，或者以 **-----BEGIN EC PRIVATE KEY-----** 开头，并以 **-----END EC PRIVATE KEY-----** 结尾的ECC算法私钥。

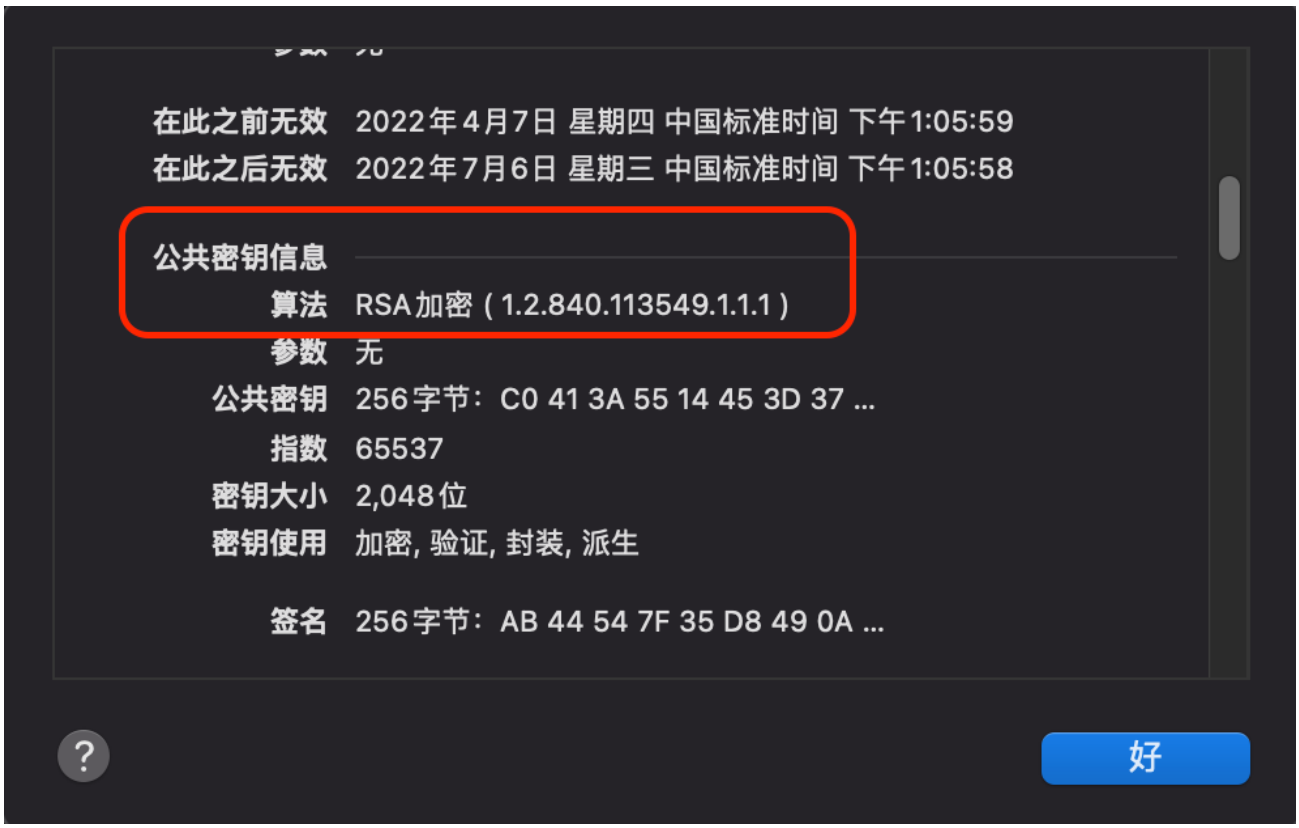
所以，当所上传证书的私钥格式为通用PEM格式时，需要手动将其转换为对应算法的私钥。

解决方案

1. 获取证书私钥文件的算法类型。下文将介绍两种获取方式，任选一种执行即可：

   - 直接查看证书详情：

     在本地计算机中，双击打开该证书文件后，在详情中查看公共密钥的算法，该算法即为对应私钥的算法类型。

   - 通过命令行查看证书详情：

     通过OpenSSL命令行工具，查看证书详情，其中 **Public Key Algorithm** 参数的值即为对应私钥的算法类型。具体命令如下：

     ```
     openssl x509 -in <证书文件路径> -noout -text
     ```

```
[root@centos import-cert-test]#
[root@centos import-cert-test]#
[root@centos import-cert-test]# openssl x509 -in cert.pem -noout -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            04:01:77:aa:ff:ce:3a:94:5d:fe:87:3e:1b:22:25:42:e7:6f
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Let's Encrypt, CN=R3
        Validity
            Not Before: Apr  7 05:05:59 2022 GMT
            Not After : Jul  6 05:05:58 2022 GMT
        Subject: CN=*.easystack.cn
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c0:41:3a:55:14:45:3d:37:77:cb:60:59:14:b3:
                    c1:c9:1a:71:13:c4:cf:2c:f7:30:18:20:70:85:36:
                    07:60:7c:f2:fe:dd:de:b7:8b:3e:5c:42:3c:76:52:
                    e0:1d:75:4c:51:52:fd:f0:0d:84:57:fc:50:8d:c7:
                    a5:96:56:05:02:6b:c2:bc:ea:14:b0:16:f9:a2:36:
```

2. 转换证书私钥文件为对应算法私钥。

通过OpenSSL命令行工具，将该证书的通用格式私钥文件转换为对应算法私钥文件。具体命令如下：

```
openssl <私钥算法> -in <通用格式私钥文件路径> -out <对应算法私钥文件路径>
```

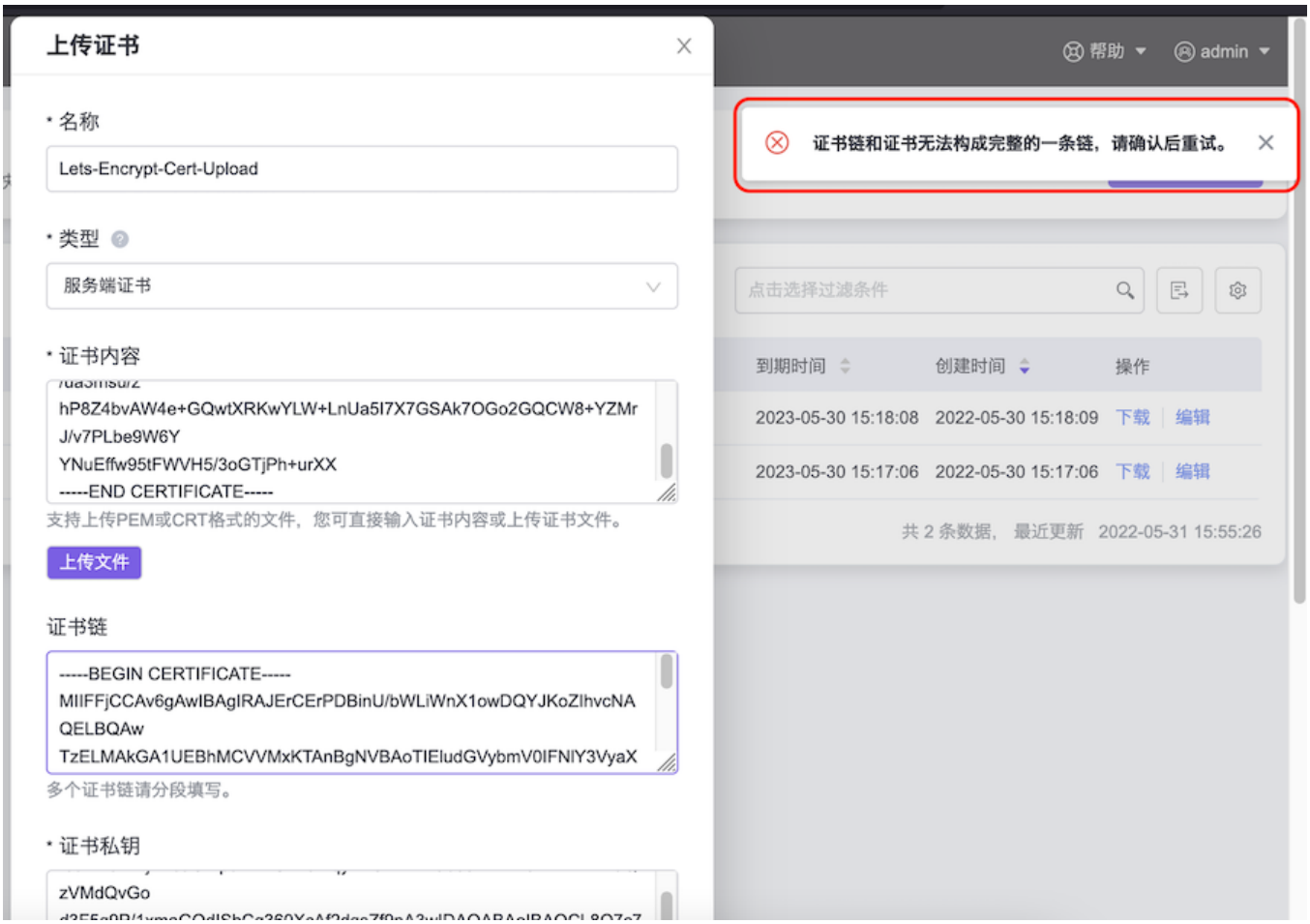
参数	说明
私钥算法	证书对应私钥的算法，即上一步骤中所获取到的算法。 当算法类型为RSA时，该参数值为 **rsa**。当算法类型为ECC时，该参数值为 **ec**。
通用格式私钥文件路径	转换前证书私钥文件的路径。

参数	说明
对应算法私钥文件路径	转换后证书私钥文件的路径。

1.4 当上传Let's Encrypt颁发证书时，提示证书链校验失败，如何排查解决

问题描述

证书与密钥服务云产品支持将第三方生成的证书上传至云平台，进行统一存储与管理，有效提高证书运维效率。但是，当上传Let's Encrypt颁发的证书时，可能提示“证书链和证书无法构成完整的一条链，请确认后重试”。



问题原因

证书与密钥服务云产品要求所上传证书的证书链正确且完整，而Let's Encrypt颁发的证书，在下载后证书包中证书链信息可能是不正确的，需要手动处理后再上传。

在Let's Encrypt颁发的证书中，证书包内包含文件如下：

- cert.pem：所申请的服务器证书，可以直接上传至“上传证书”对话框的“证书内容”参数中。
- privkey.pem：服务器证书所对应的私钥文件。该私钥文件为通用PEM格式，需参考 当上传证书时提示私钥格式校验失败，如何排查解决 转换为对应算法格式后，再上传至“上传证书”对话框的“证书私钥”参数中。
- chain.pem：签发服务器证书的CA证书链。该证书链中根CA的证书可能不正确，需获取正确根CA的证书，再上传至“上传证书”对话框的“证书链”参数中。
- fullchain.pem：包含签发服务器证书的CA证书链和服务器证书。

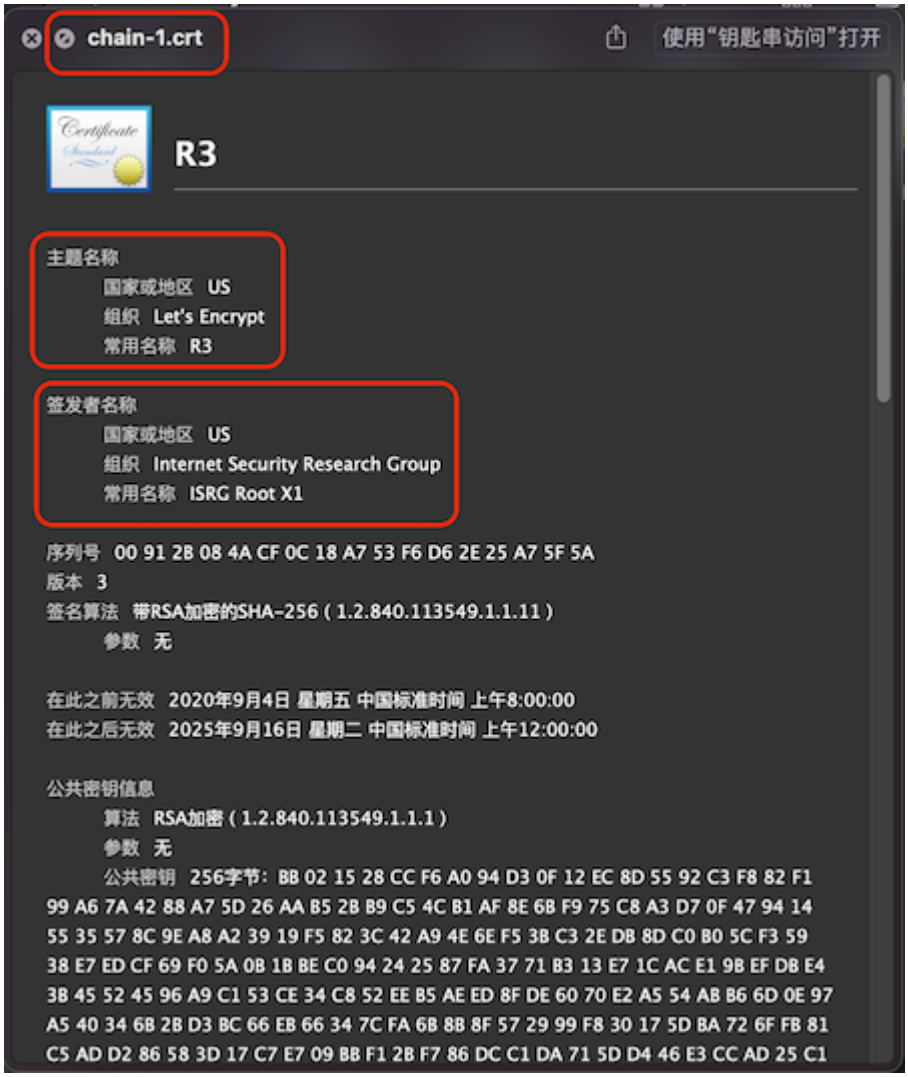
解决方案

1. 通过文本编辑器打开chain.pem文件，依次将该文件中以 **-----BEGIN CERTIFICATE-----** 开头，并最小范围内以 **-----END CERTIFICATE-----** 结尾的一段内容，复制到一个独立文件中，且命名为 *chain-X.crt* 格式，以作为一个CA证书。
2. 提取Let’s Encrypt CA证书。依次双击打开上述CA证书，以确认Let's Encrypt的证书文件，该CA证书内容即为所上传证书的证书链部分内容。

   下文将介绍两种常见操作系统确认Let's Encrypt证书文件的具体方法，请根据实际操作环境执行对应操作：

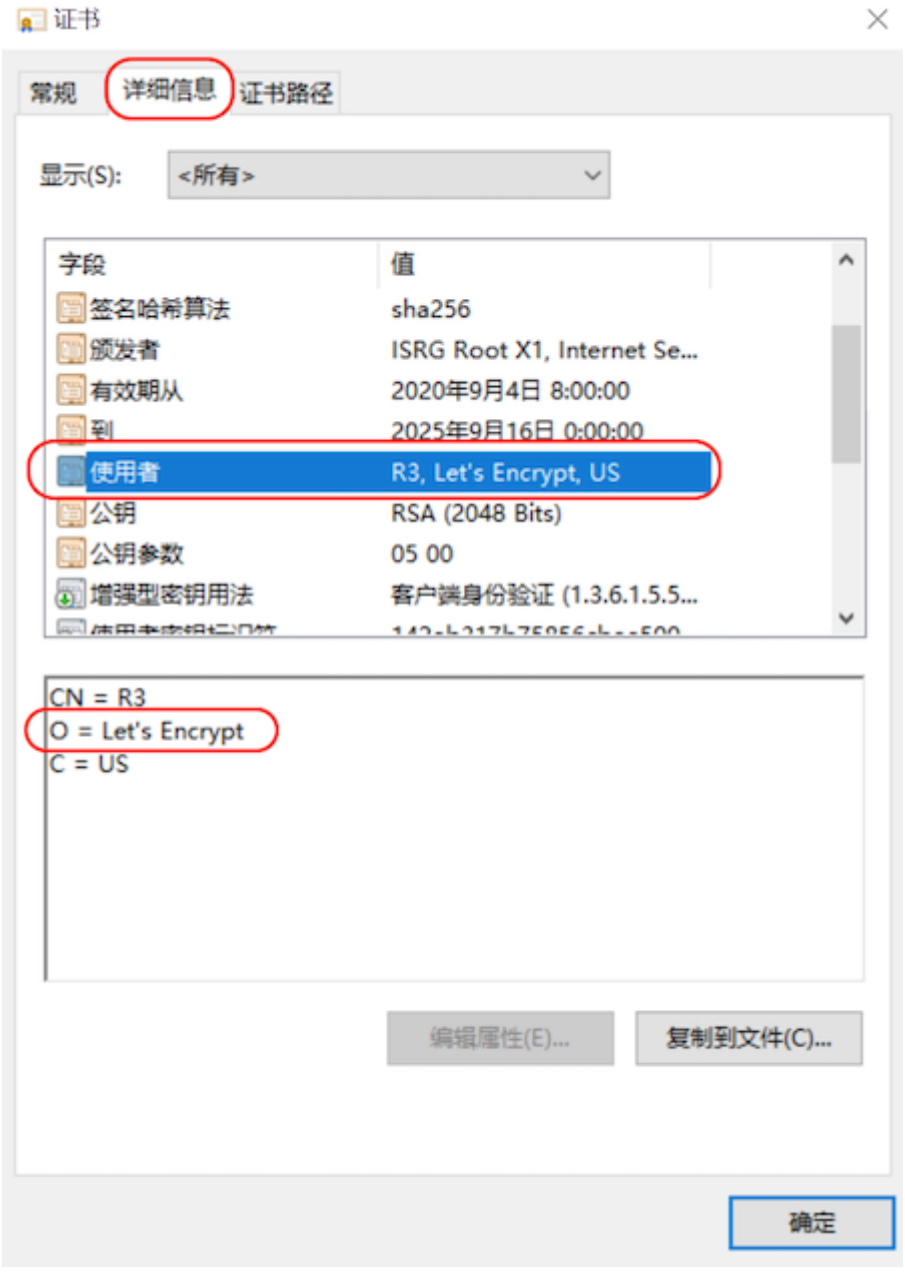
   - Mac操作系统：

     在“主题名称”区域框下，“组织”为 **Let’s Encrypt** 的CA证书。



- Windows操作系统：

  在 [详细信息] 页签中，“使用者”为 **Let's Encrypt** 的CA证书。



3. 提取根CA证书。根CA文件内容即为所上传证书的证书链剩余内容。下文将介绍两种常见操作系统的具体提取方法，请根据实际操作环境执行对应操作：

   - Mac操作系统：

     1. 在本地计算机中，打开“钥匙串访问”窗口。之后，在左导航中选择 [系统根证书]，并在页面上方选择 [证书]页签，进入“证书”页面。

     2. 在 **ISRG Root X1** 所在行右键单击后，在右键菜单中选择 `导出“ISRG Root X1”` ，将其存储至本地（文件格式请选择“增强保密邮件(.pem)”）。

- Windows操作系统：

  1. 在本地计算机中，通过按 `Win` + `R` 键，打开“运行”窗口。之后，输入“certmgr.msc”，进入“证书”页面。

  2. 在左侧导航栏中，选择 [受信任的根证书颁发机构]-[证书]后，在右侧显示页面中右键单击 **ISRG Root X1** 所在行后，在右键菜单中选择 `所有任务` - `导出` 后，按提示将其导出存储至本地（文件格式请选择“Base64 编码 X.509(.CER)(S)”）。

4. “上传证书”对话框中“证书链”参数的值即为 **Let’s Encrypt CA证书文件内容** + **根CA证书文件内容** ，二者之间通过换行分隔开即可。

咨询热线：400-100-3070

北京易捷思达科技发展有限公司：
北京市海淀区西北旺东路10号院东区23号楼华胜天成科研大楼一层东侧120-123
南京分公司：
江苏省南京市雨花台区软件大道168号润和创智中心B栋一楼西101
上海office：
上海黄浦区西藏中路336号华旭大厦22楼2204
成都分公司：
成都市高新区天府五街168号德必天府五街WE602

邮箱：
contact@easystack.cn (业务咨询)
partners@easystack.cn(合作伙伴咨询)
marketing@easystack.cn (市场合作)
training@easystack.cn (培训咨询)
hr@easystack.cn (招聘咨询)