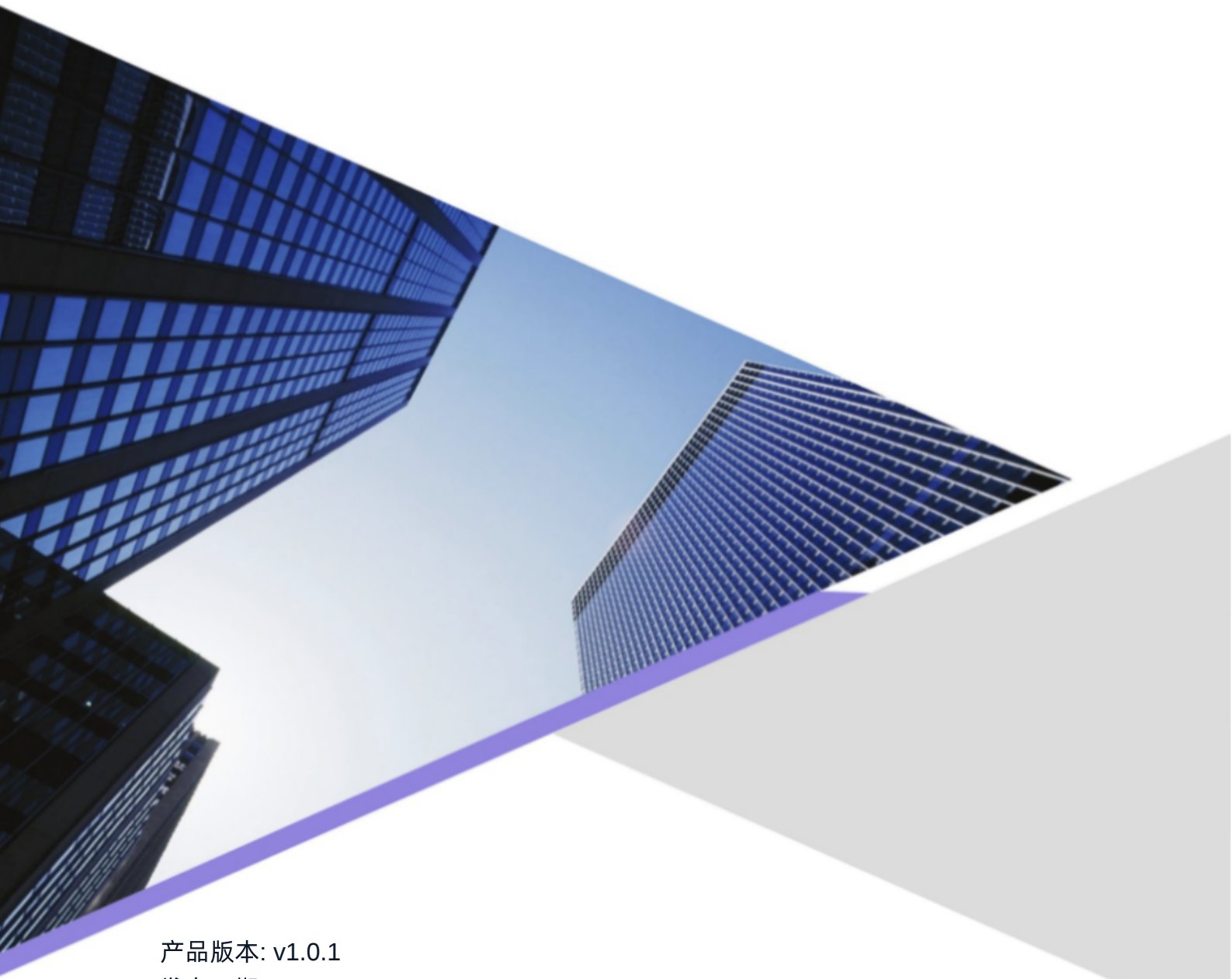
EasyStack
易捷行云

证书服务

常见问题



产品版本: v1.0.1
发布日期: 2025-07-09

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。

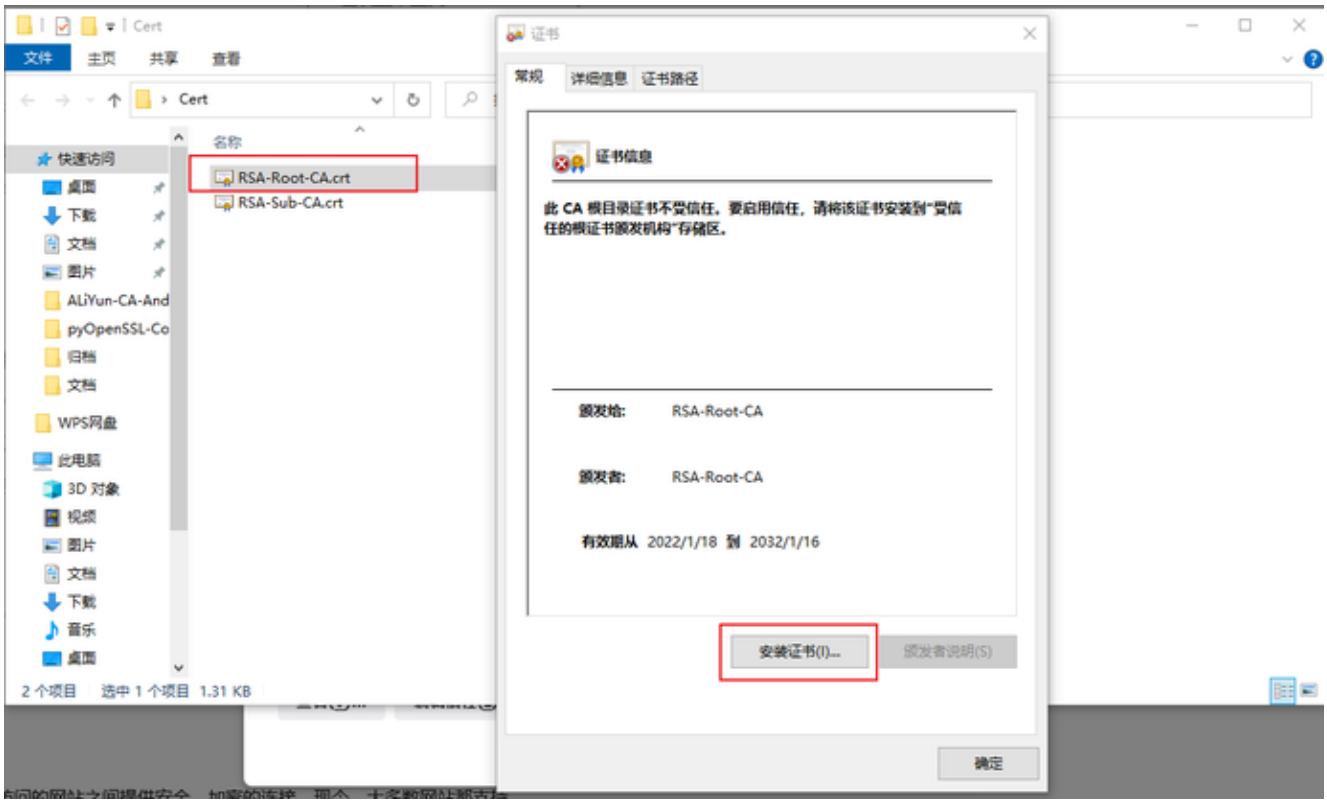
> 说明：
> Firefox浏览器是从浏览器内部的证书库检查当前证书的签发CA是否受浏览器信任，而不是读取操作系统中的证书库，因此其配置方式不同于其它浏览器。

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。

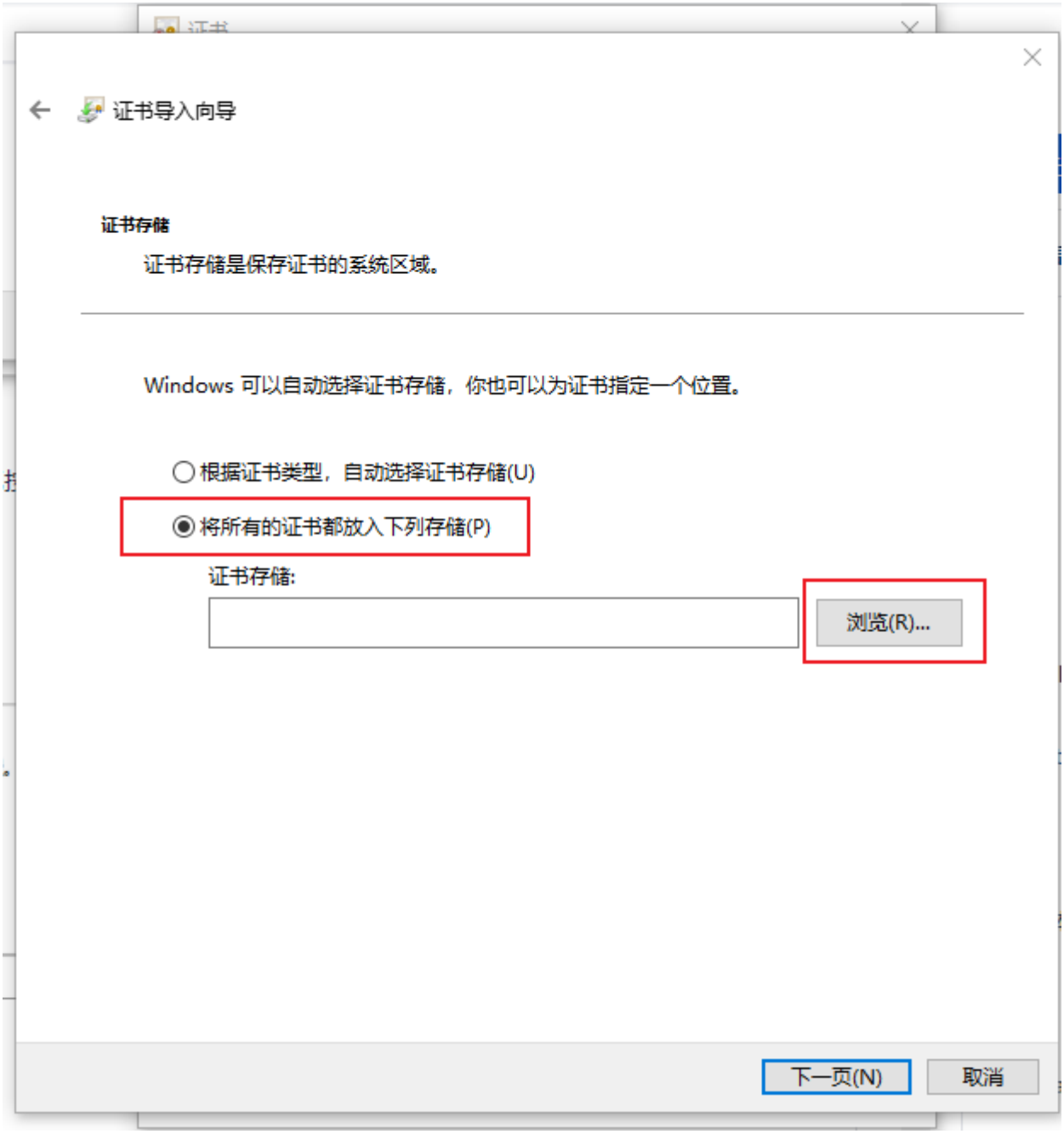
1. 在证书服务页面，下载该私有证书的签发CA链上所有的CA证书文件，即该证书的签发CA、签发CA的上一级签发CA，以此类推直至根CA。

2. 双击某个CA证书文件，在弹出的窗口中单击 `安装证书` 。

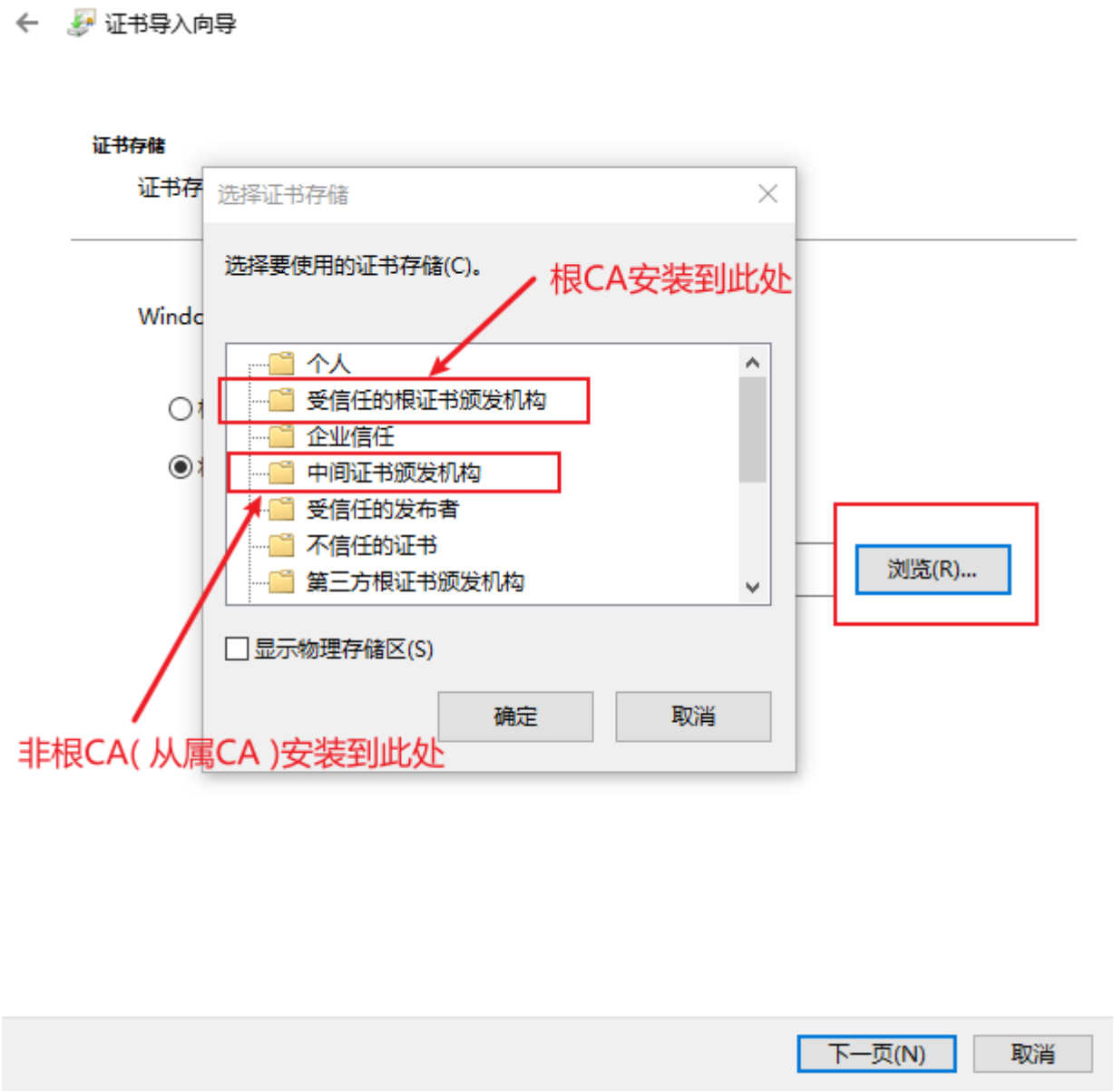


3. 存储位置选择 `当前用户` ，单击 `下一页` 。

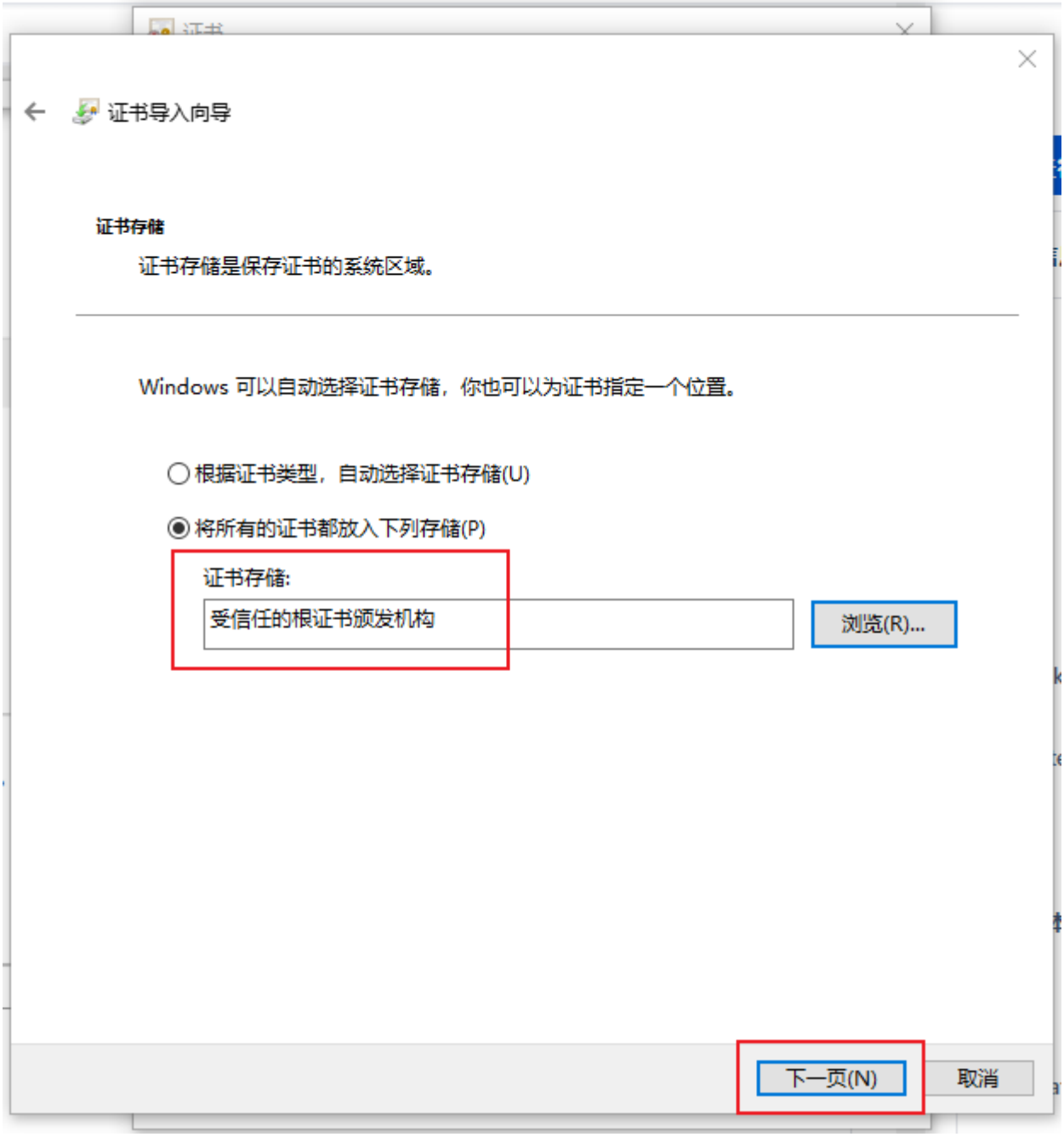
4. 选择 `将所有的证书都放入下列存储(P)` 。



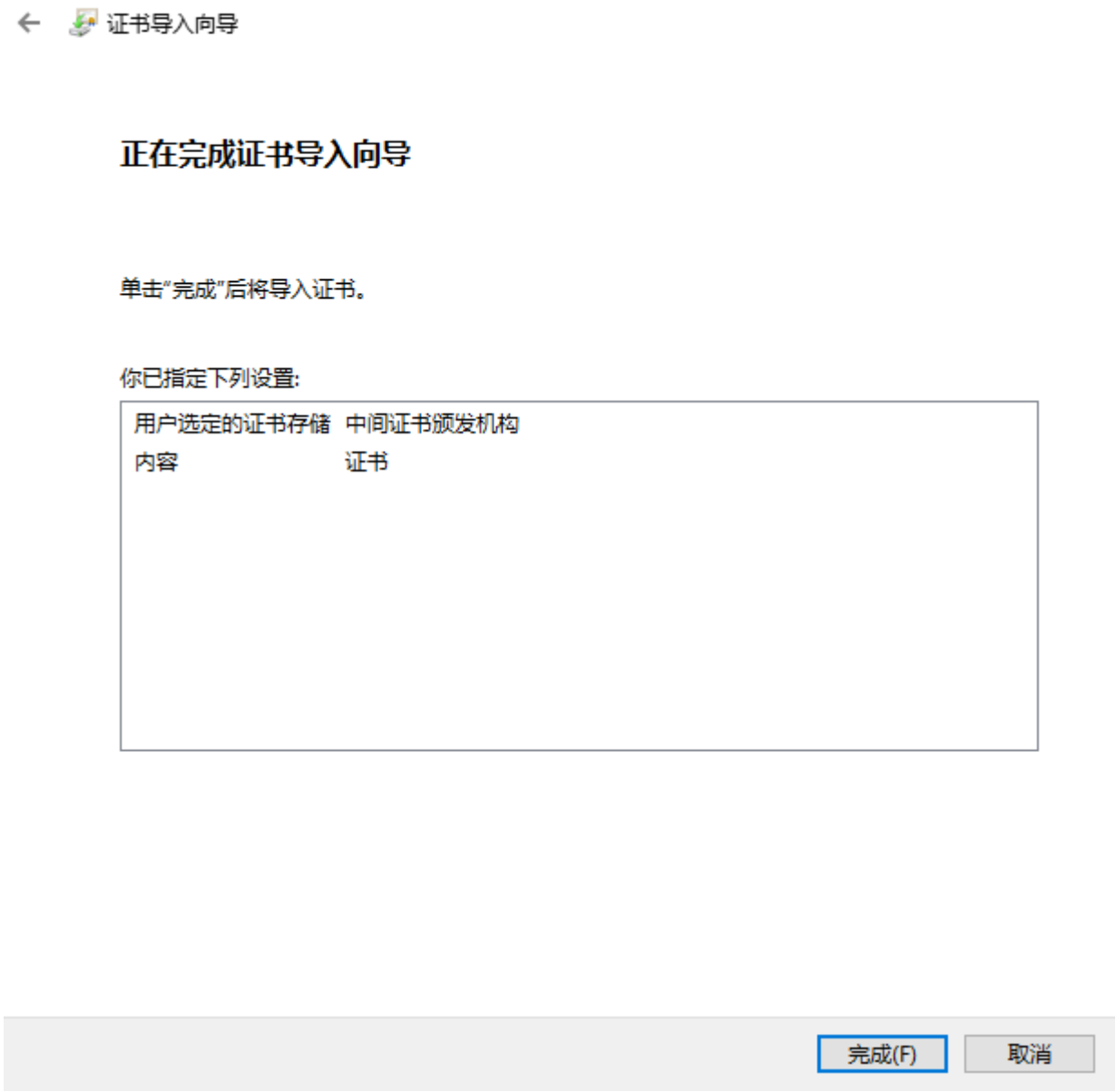
5. 单击 `浏览` ，如果是根CA选择 `受信任的根证书颁发机构` ，如果是从属CA选择 `中间证书颁发机构` 。选择完成后单击 `确定` 。


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

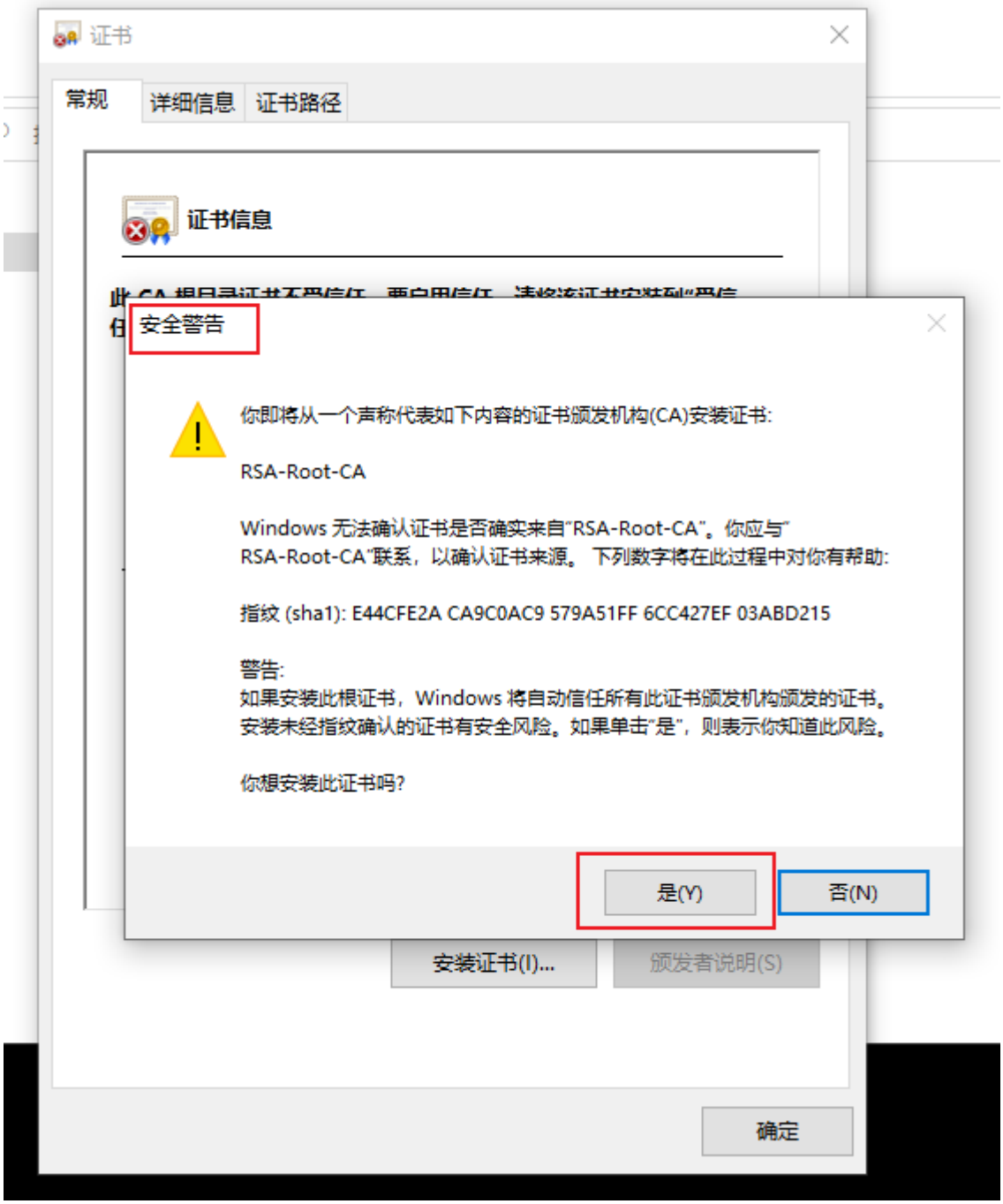
6. 单击 `下一页` 。

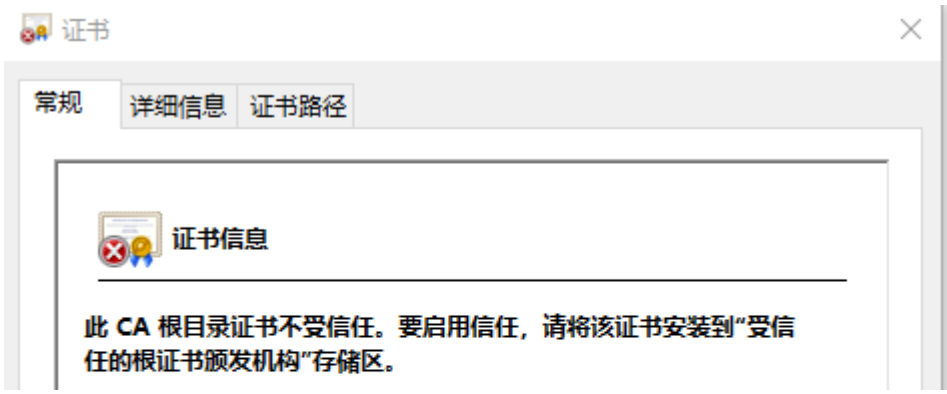


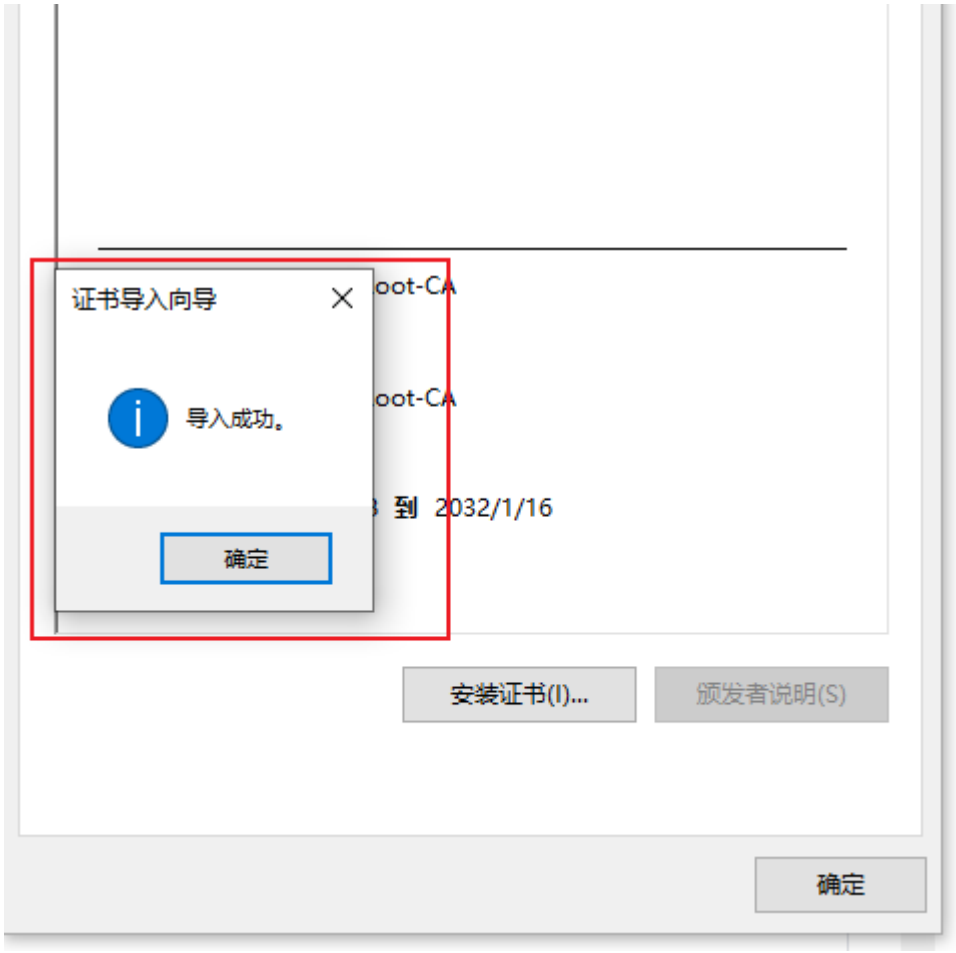
7. 单击 `完成` ，弹出安全警告窗口。


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。



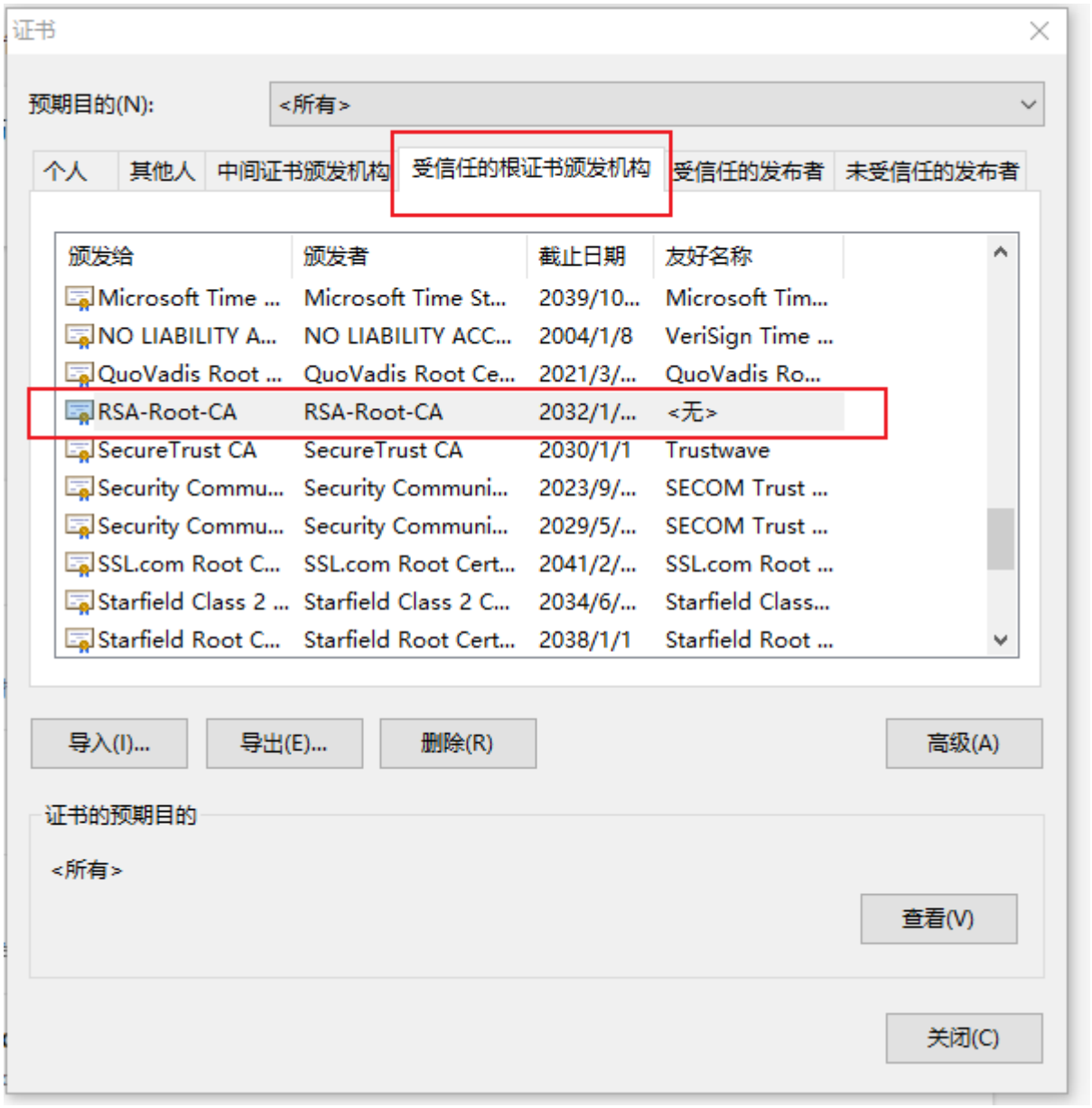
9. 重复以上步骤，依次安装该私有证书的签发CA到根CA的所有CA证书。

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。

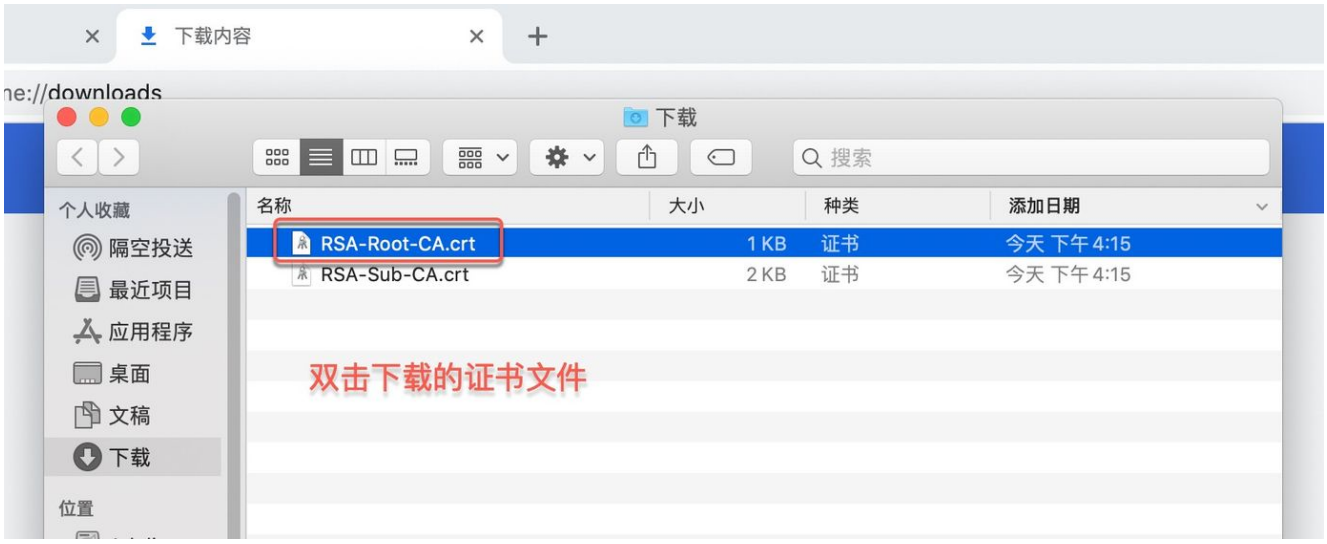


macOS操作系统

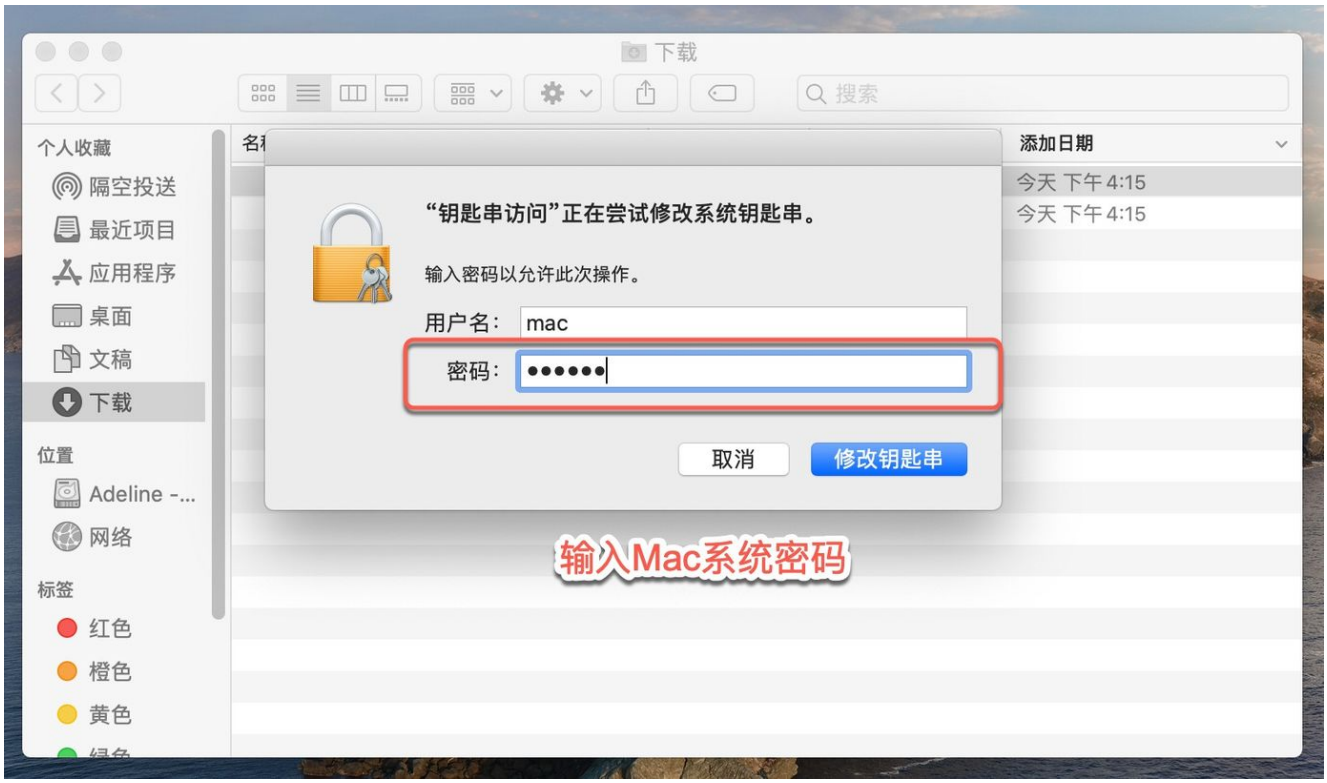
本节介绍在macOS操作系统中，如何导入私有证书的签发CA证书链，使其成为受信任的证书颁发机构。

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。

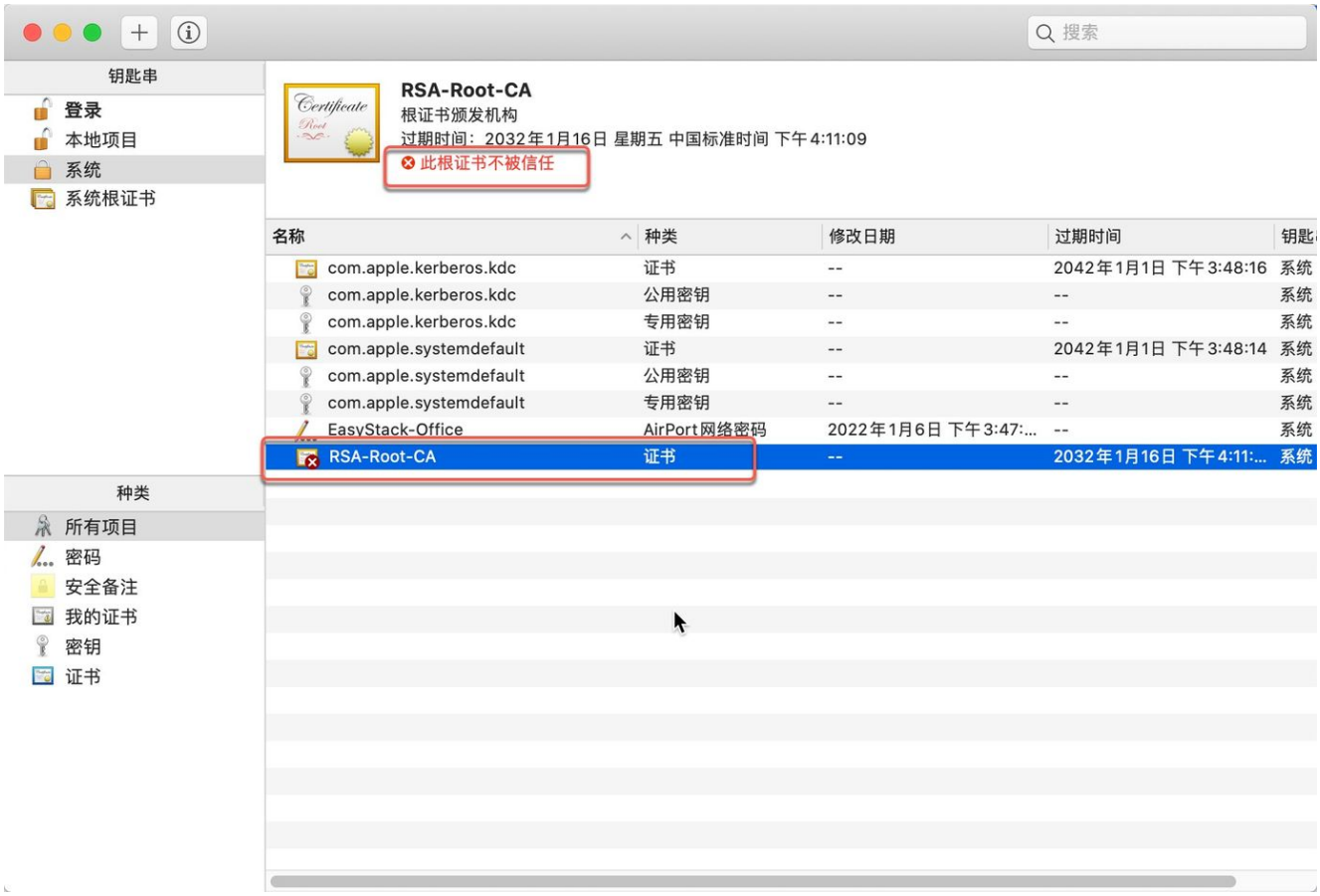
2. 双击某个证书文件，弹出密码输入窗口。



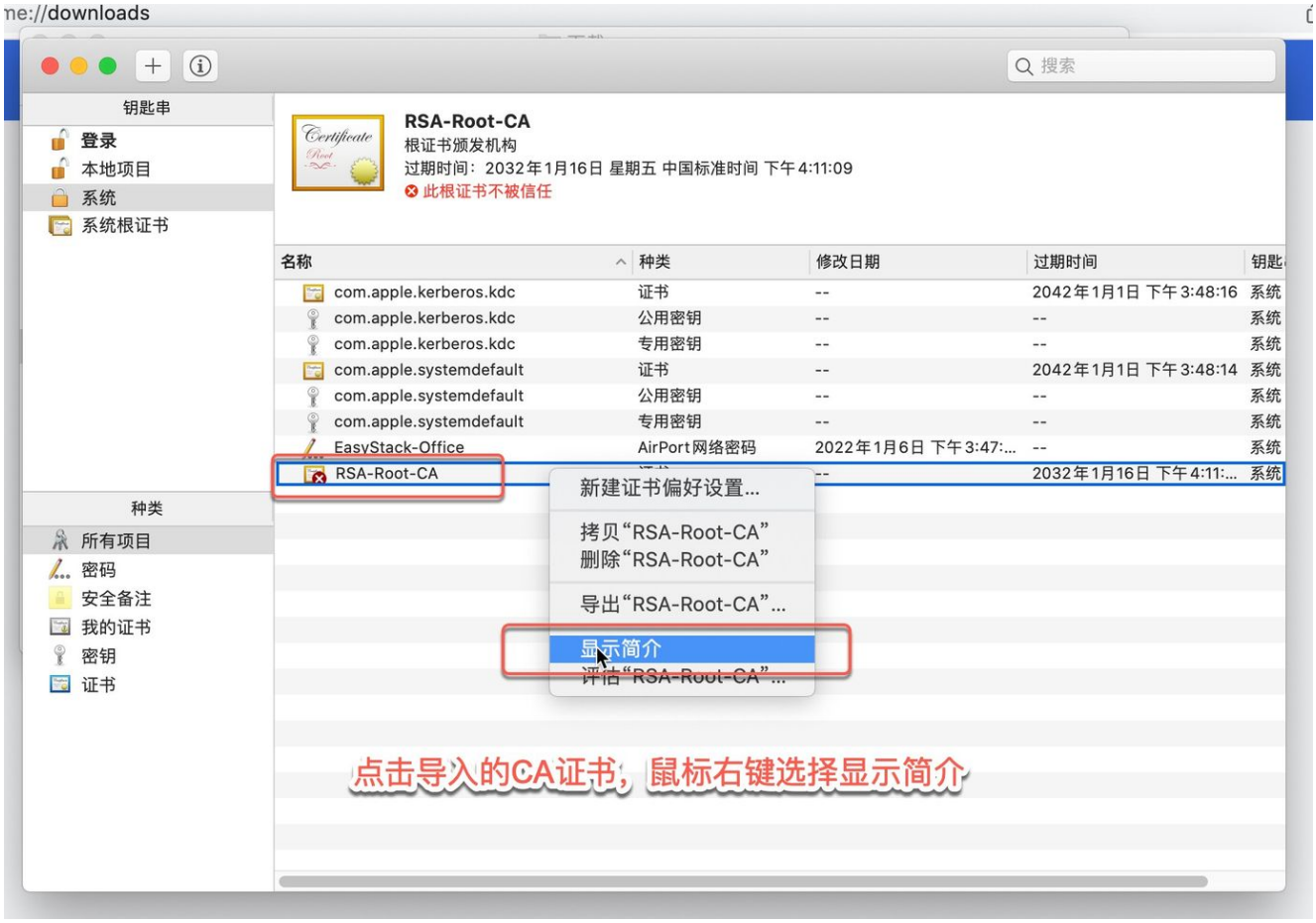
3. 输入系统密码，单击 `修改钥匙串` ，弹出钥匙串列表。



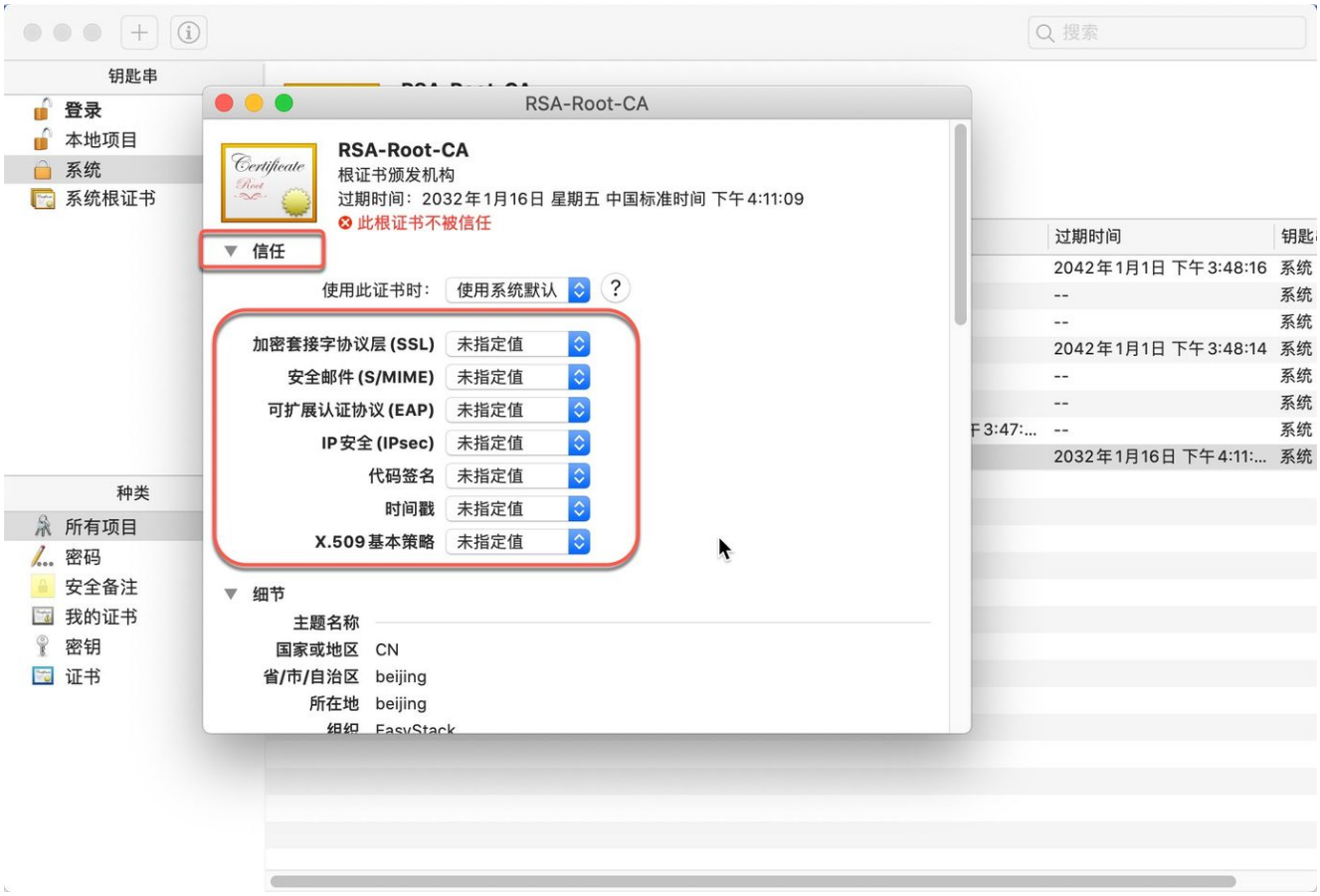
4. 此时虽然私有CA的证书已经导入到系统钥匙串中，但仍不受系统信任。



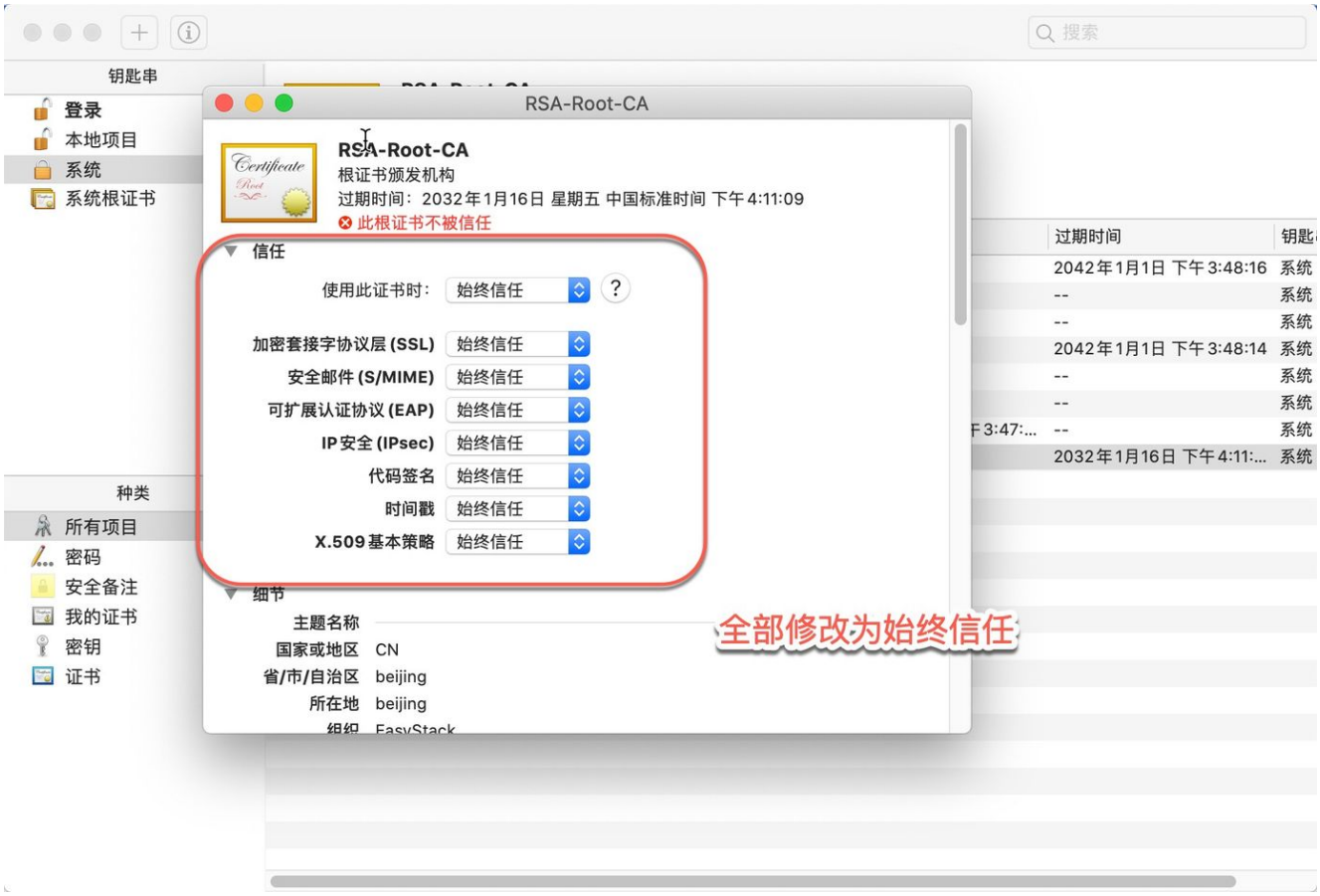
5. 右键单击导入的私有CA证书，选择“显示简介”。



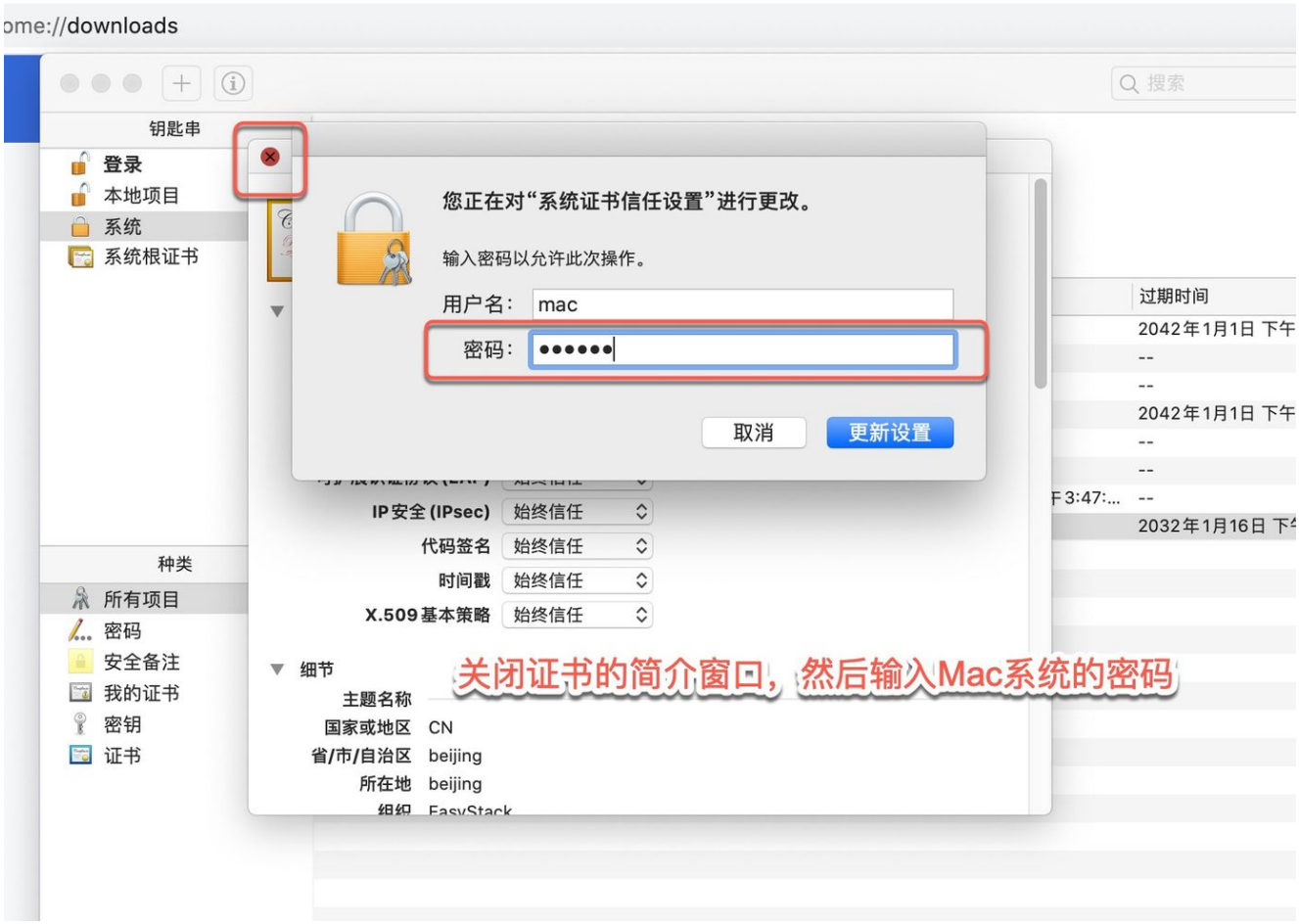
6. 展开“信任”下的详细信息。



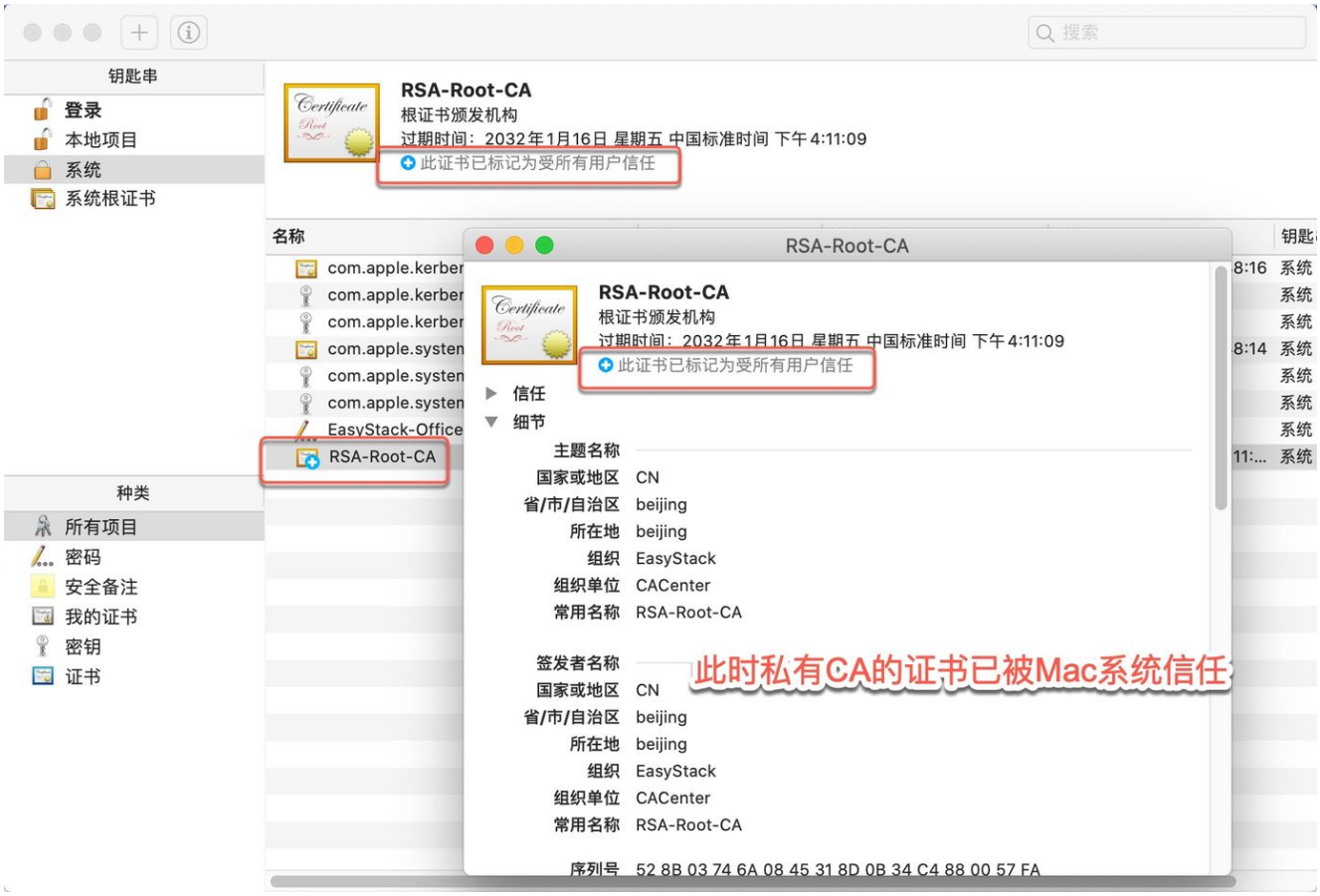
7. 将详细信息中的所有选项改为“始终信任”。



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。



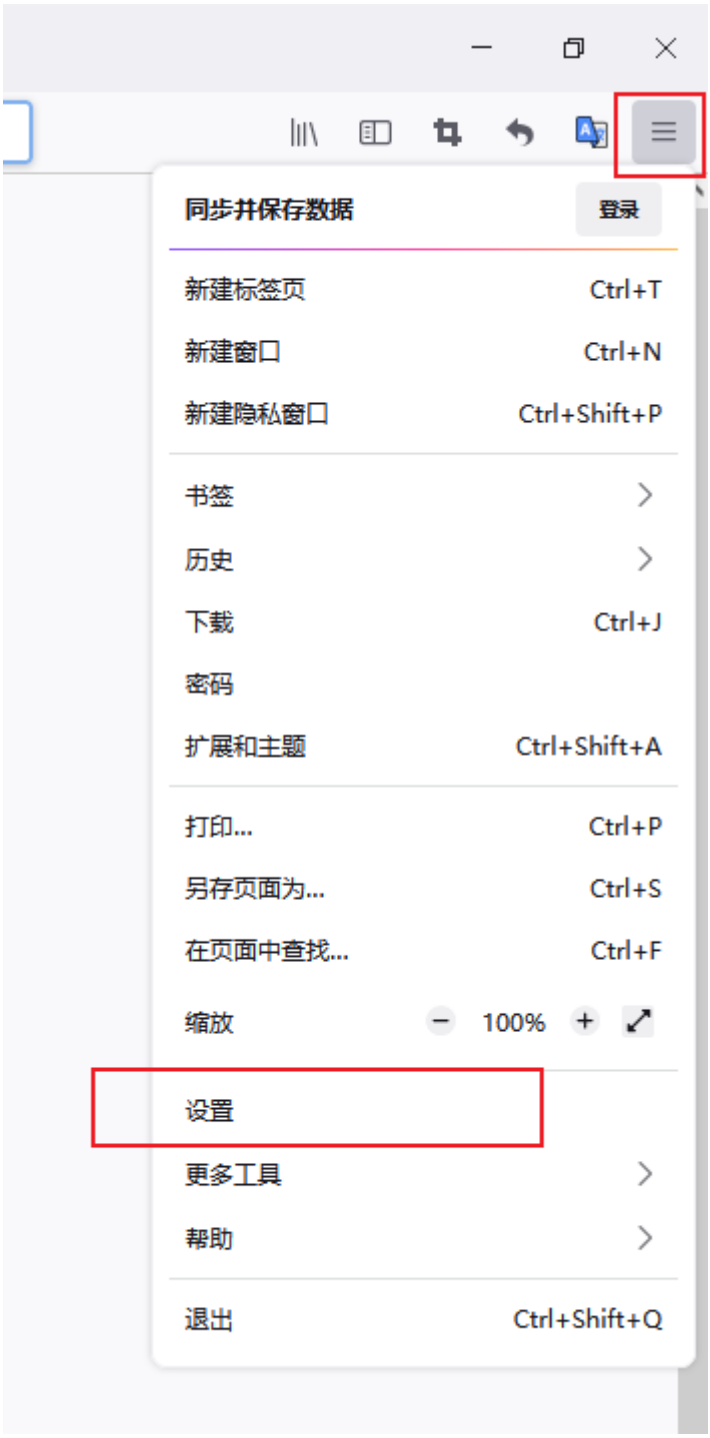
9. 再次在钥匙串列表中查看导入的私有CA证书，已被系统信任。



Firefox浏览器

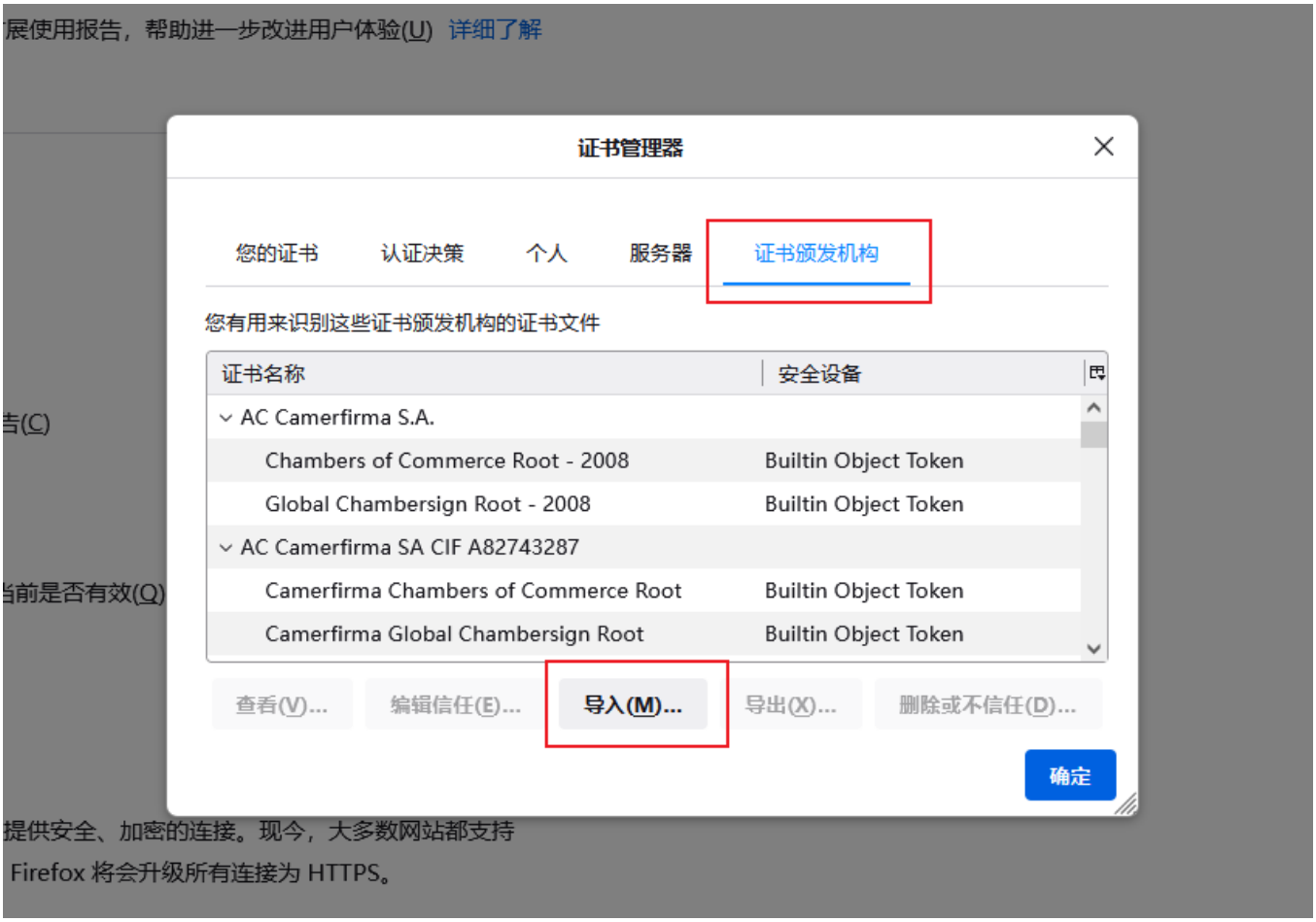
本节介绍如何在Firefox浏览器中导入私有证书的签发CA证书链，使其成为受信任的证书颁发机构。

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。

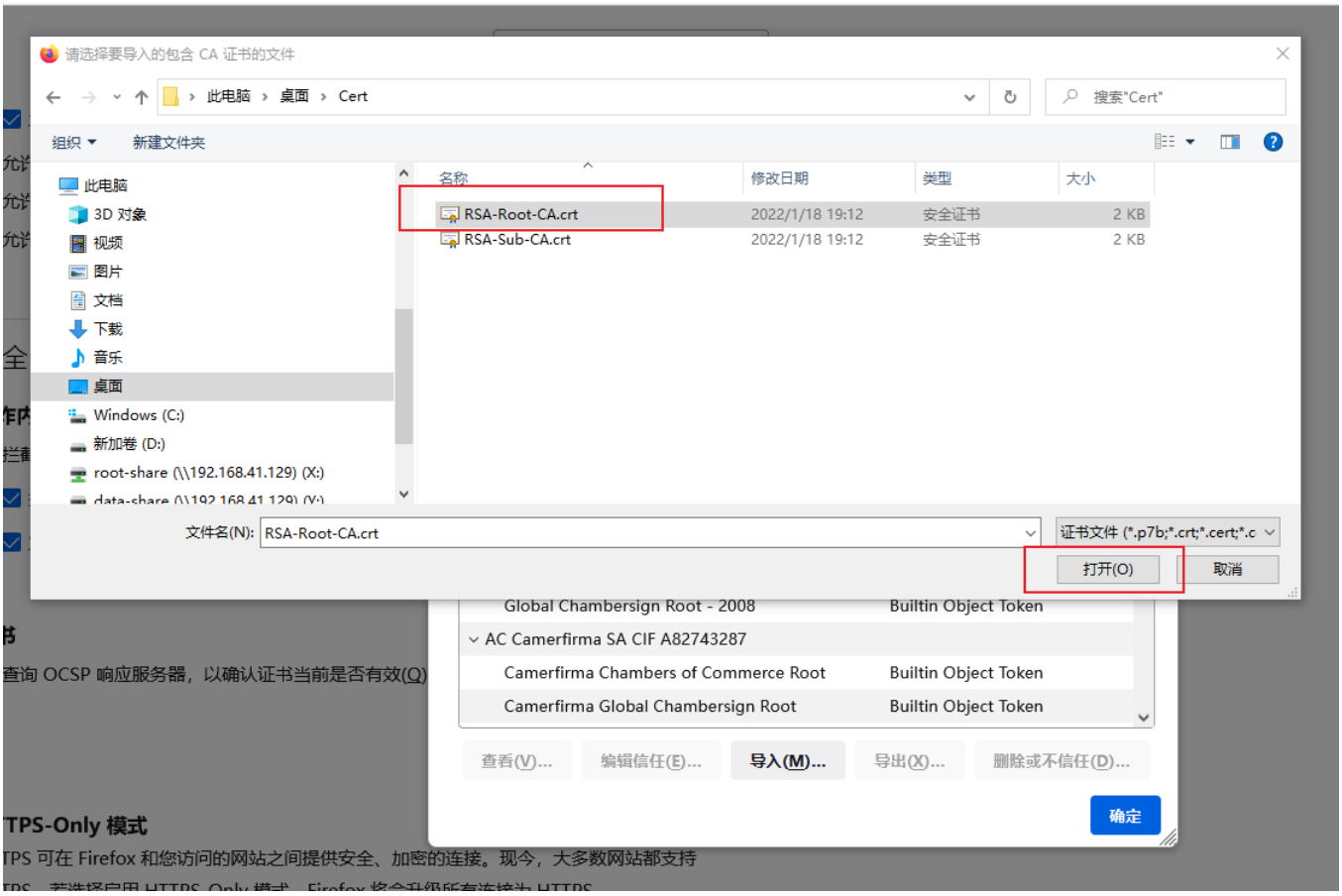


3. 在“隐私与安全”菜单项中，找到“证书”，单击 查看证书 。

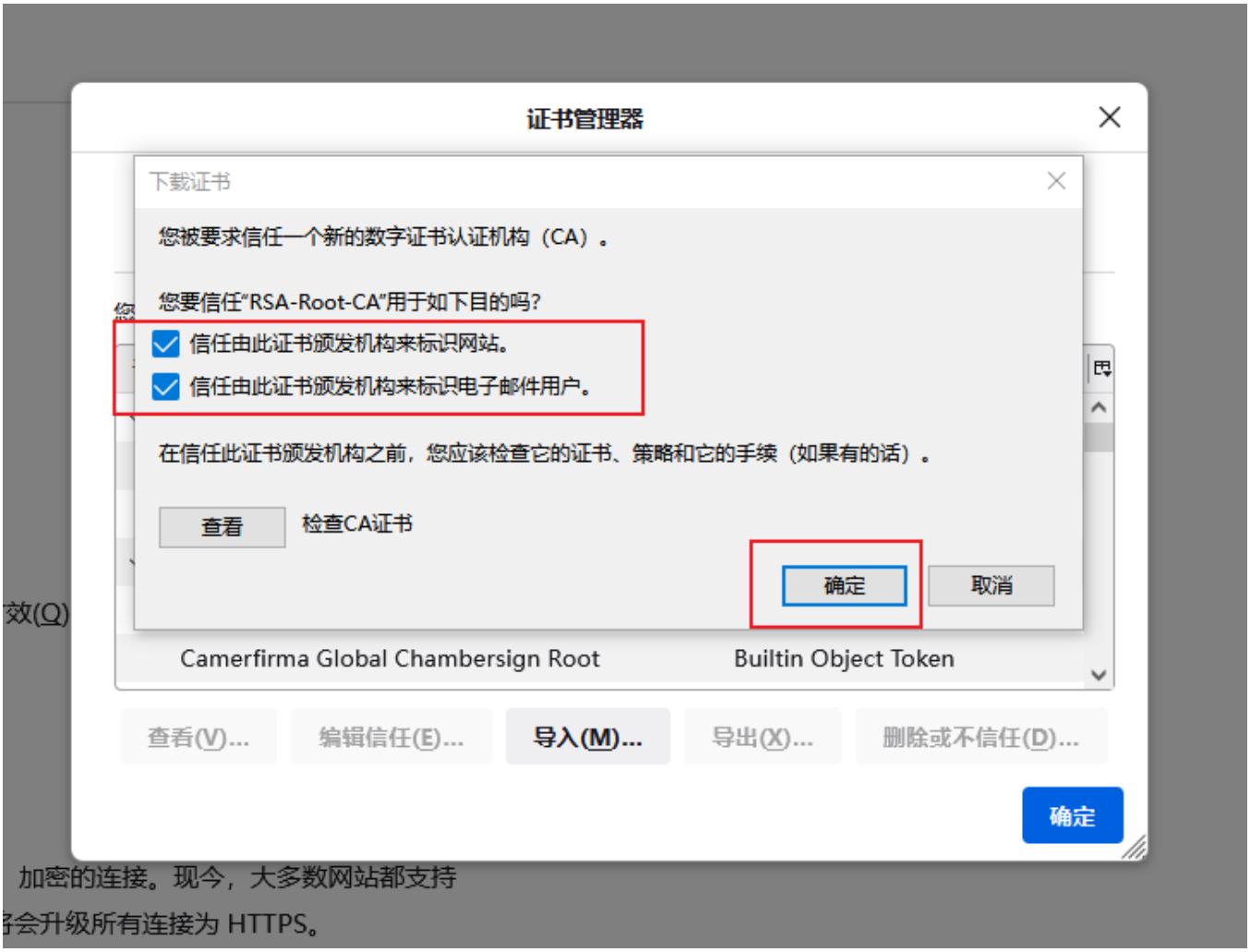
4. 在弹出的证书管理器中，选择“证书颁发机构”页签，单击 `导入` 。



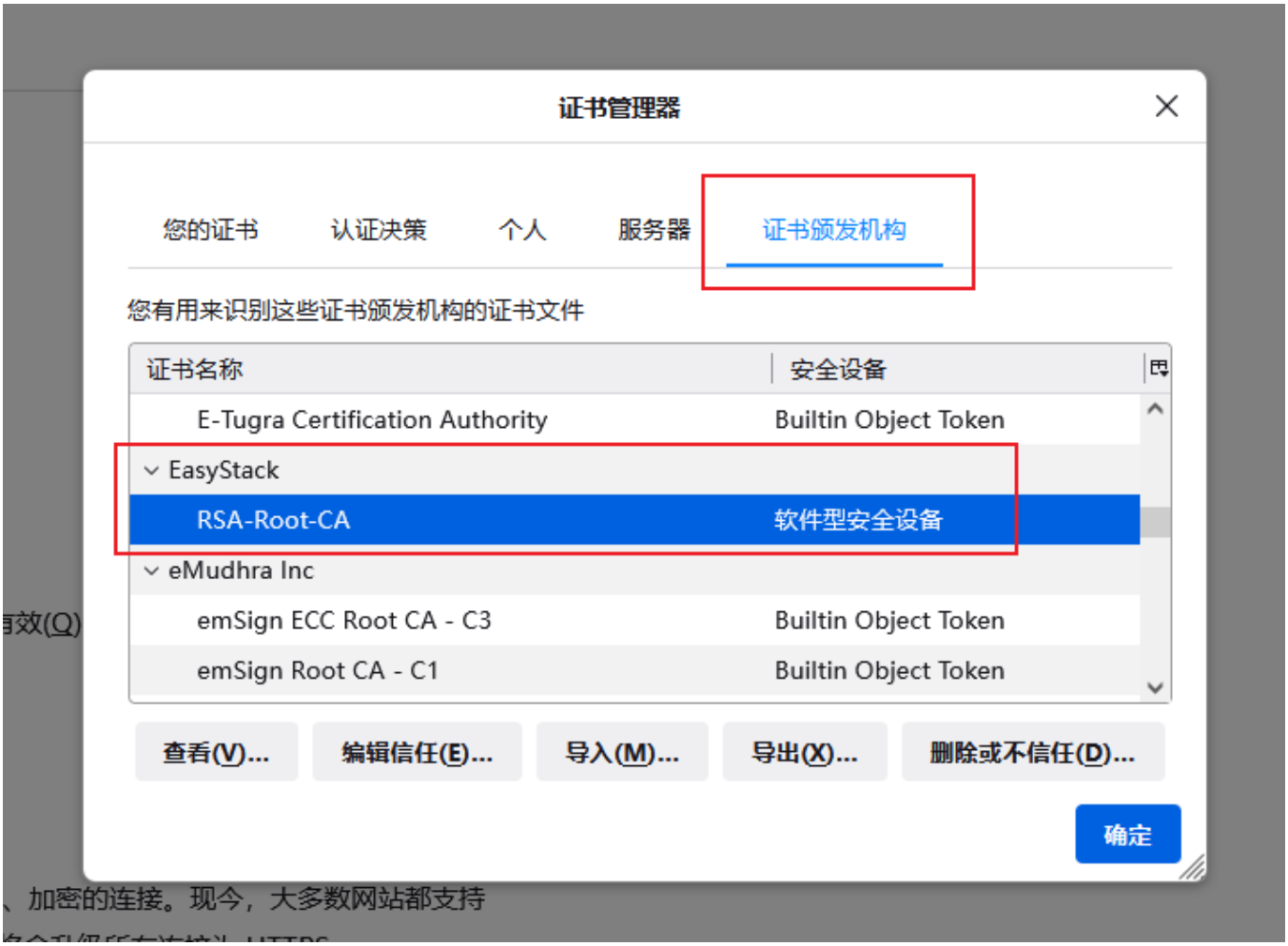
5. 选择下载好的私有CA证书文件，单击 `打开` 。



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。

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)