

# 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
1.1 客户端如何导入私有CA证书到受信任的证书颁发机构中 .....	1
1.2 服务端证书未指定域名，访问服务时提示安全风险 .....	27

# 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：



您的连接不是私密连接

攻击者可能会试图从 [qwer123.com](#) 窃取您的信息（例如：密码、通讯内容或信用卡信息）。[了解详情](#)

`NET::ERR_CERT_AUTHORITY_INVALID`

[隐藏详情](#)

[返回安全连接](#)

此服务器无法证明它是 [qwer123.com](#)；您计算机的操作系统不信任其安全证书。出现此问题的原因可能是配置有误或您的连接被拦截了。

[继续前往qwer123.com \(不安全\)](#)

### 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颁发机构中。

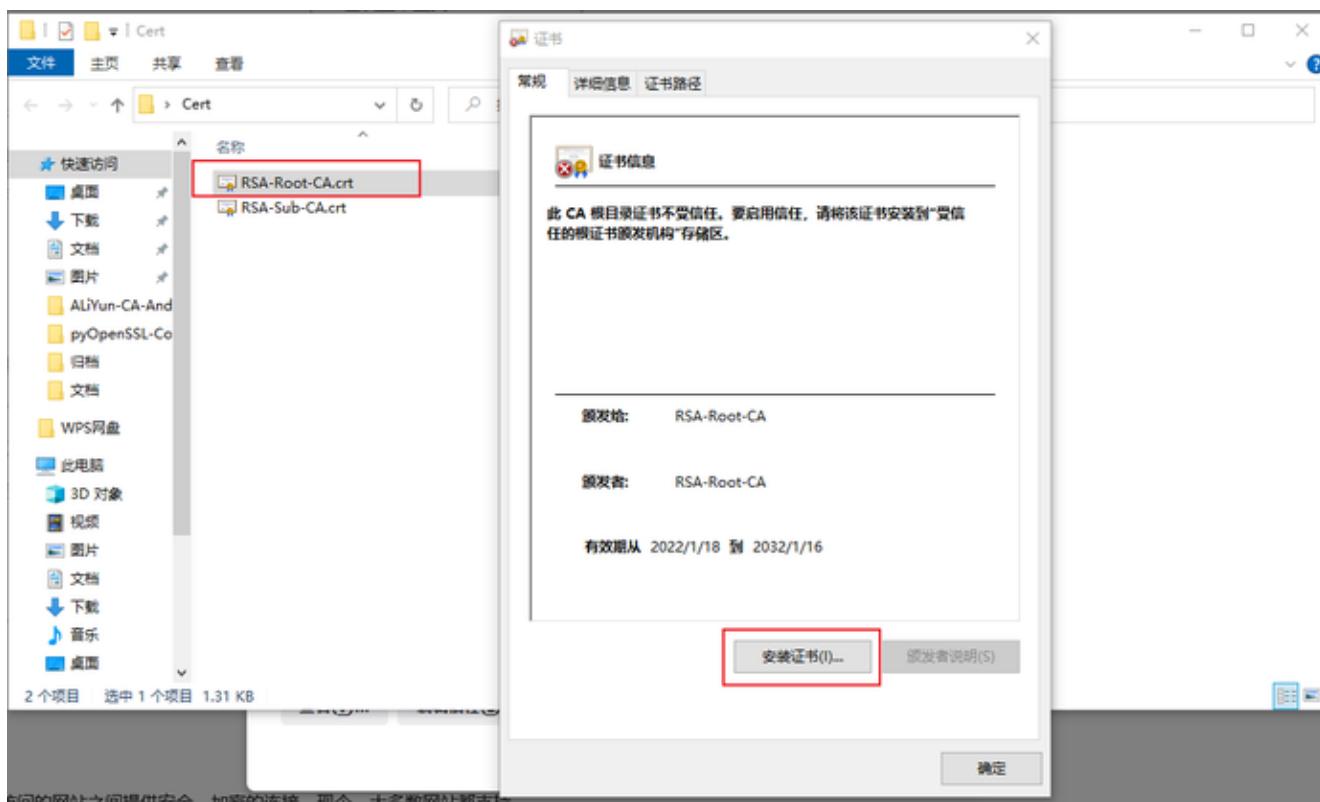
说明：

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。

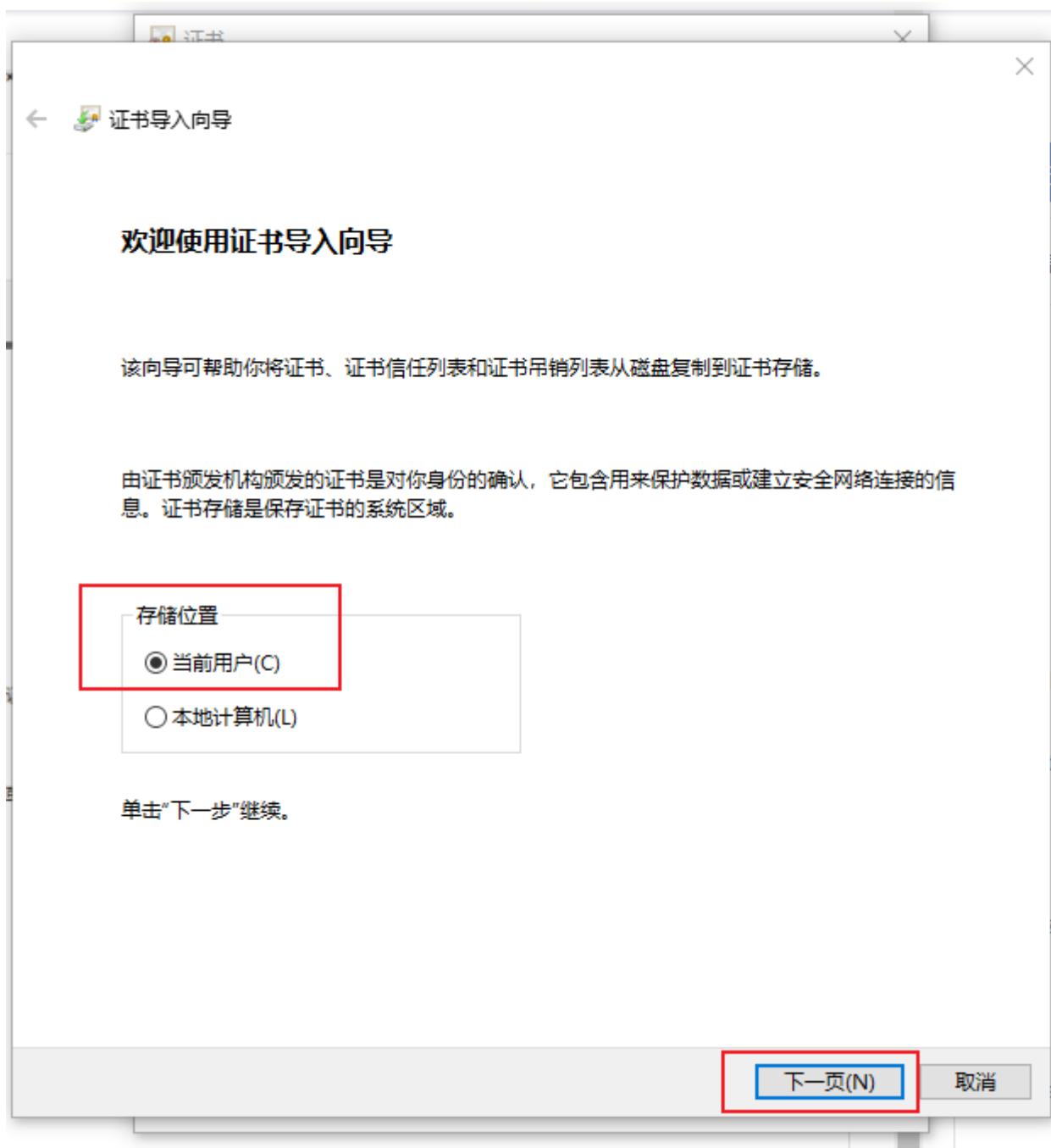
## Windows操作系统

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。

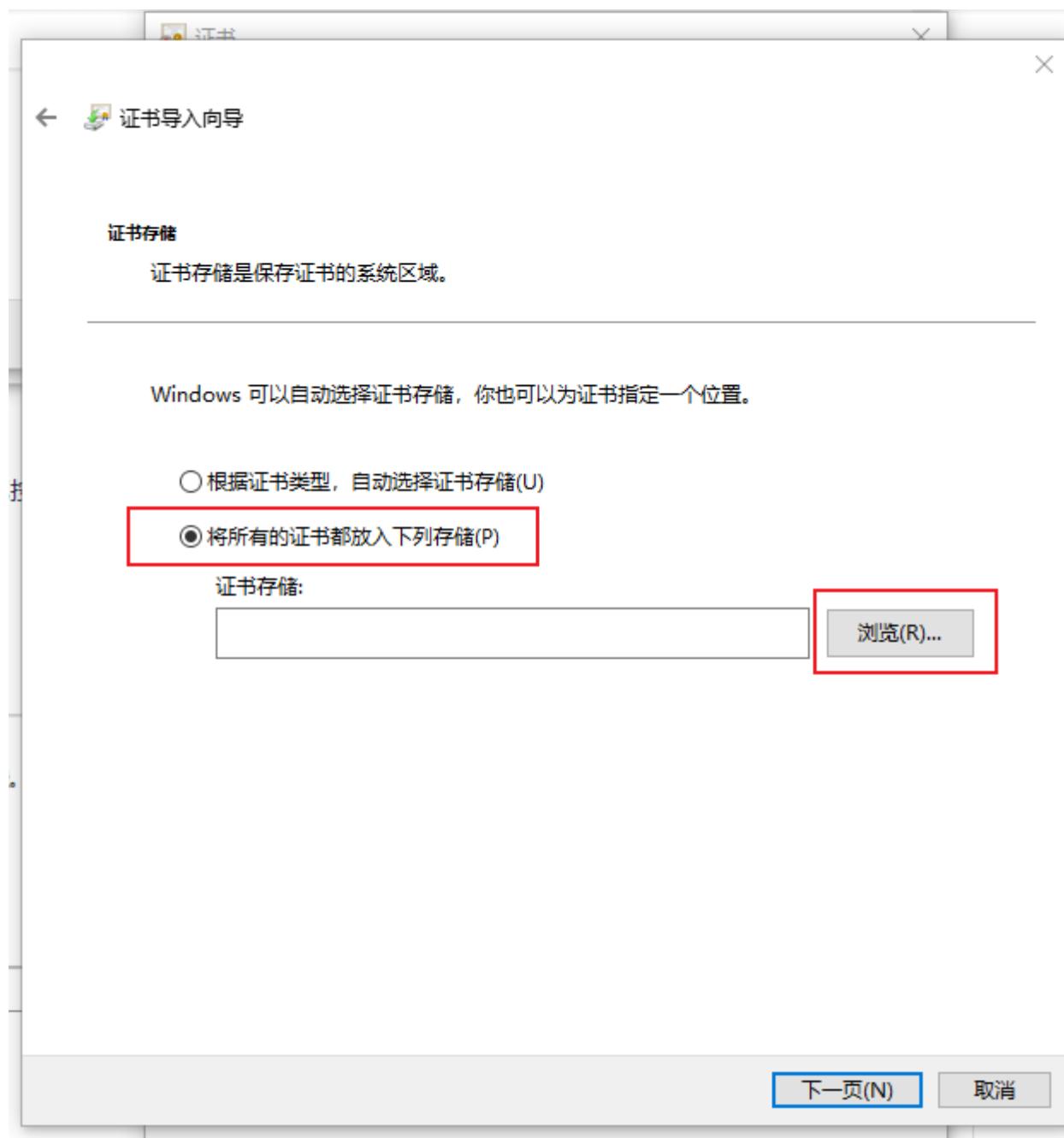
1. 在证书服务页面，下载该私有证书的签发CA链上所有的CA证书文件，即该证书的签发CA、签发CA的上级签发CA，以此类推直至根CA。
2. 双击某个CA证书文件，在弹出的窗口中单击 **安装证书**。



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

Windc

○

●

- ...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

显示物理存储区(S)

确定

取消

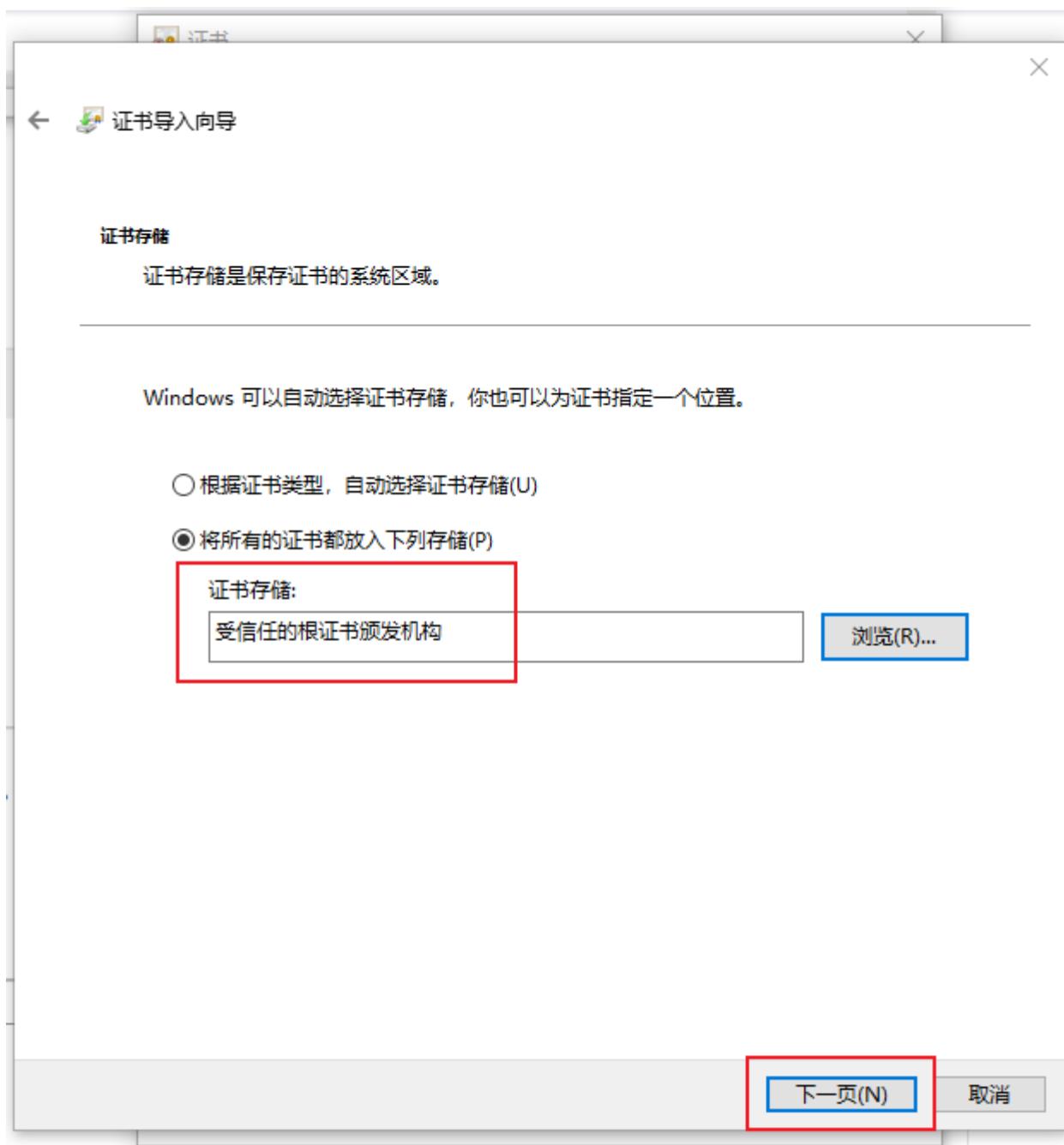
浏览(R)...

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 ，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:

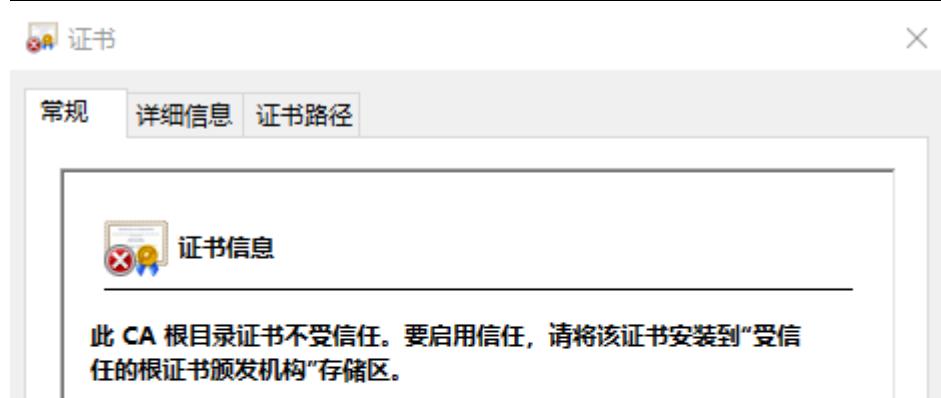
用户选定的证书存储	中间证书颁发机构
内容	证书

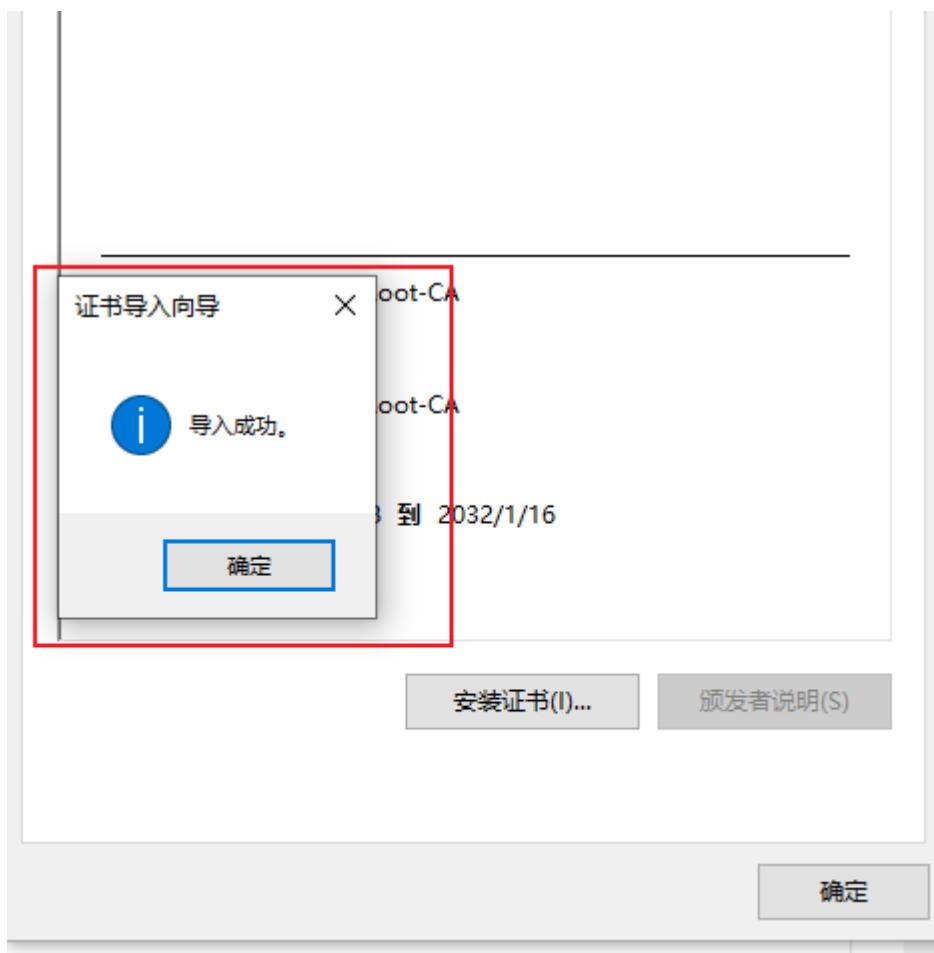
完成(F)

取消

8. 单击 **是**，提示导入成功。







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。

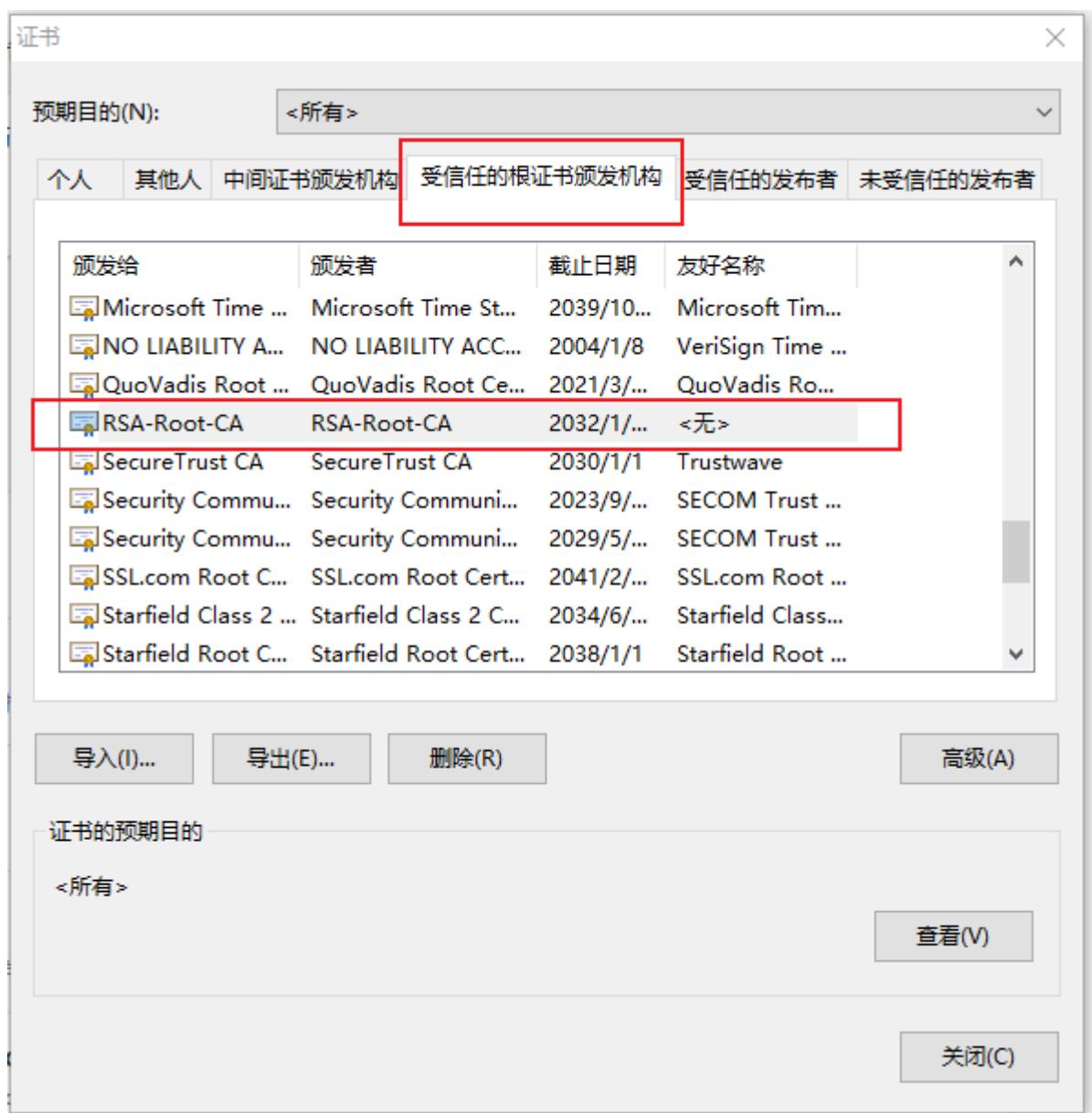


2. 在“隐私、搜索和服务”菜单项中找到“安全性”，单击“管理证书”。



The screenshot shows the Microsoft Edge settings interface. On the left, a sidebar lists various settings categories. The 'Privacy, search and services' option is highlighted with a red box. On the right, the main content area is titled '个性化你的 Web 体验' (Personalize your Web experience) and contains a toggle switch for allowing Microsoft to use browsing history to improve ads, search, news, and other services. Below this is a 'Security' section with a red box around the 'Management Certificates' subsection. This subsection includes options for managing HTTPS/SSL certificates and using Microsoft Defender SmartScreen.

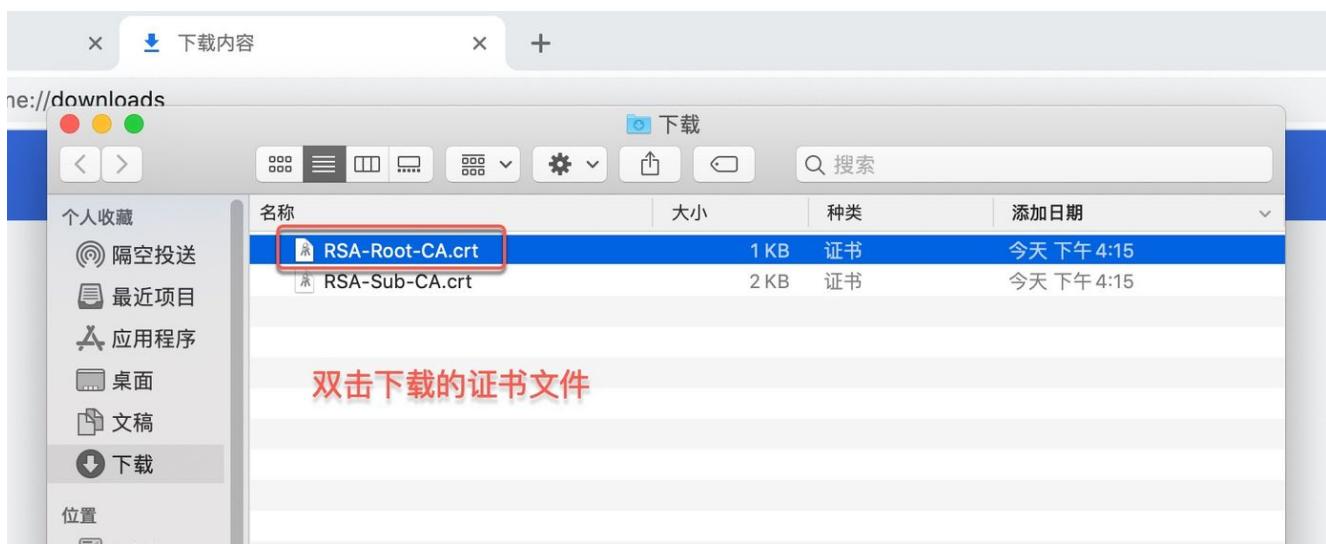
3. 在弹出的证书窗口中，查看“受信任的根证书颁发机构”和“中间证书颁发机构”页签，即可查看到导入的根CA证书和从属CA证书。



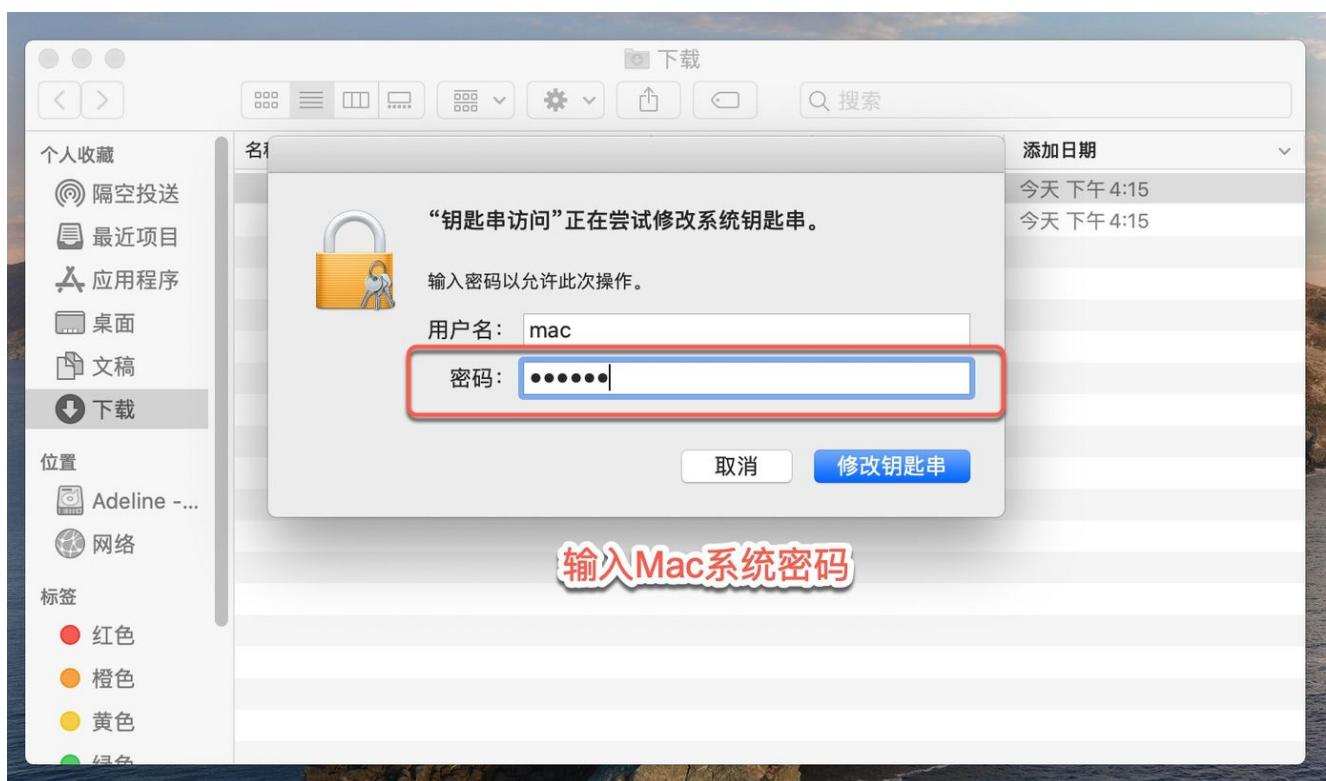
## macOS操作系统

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。

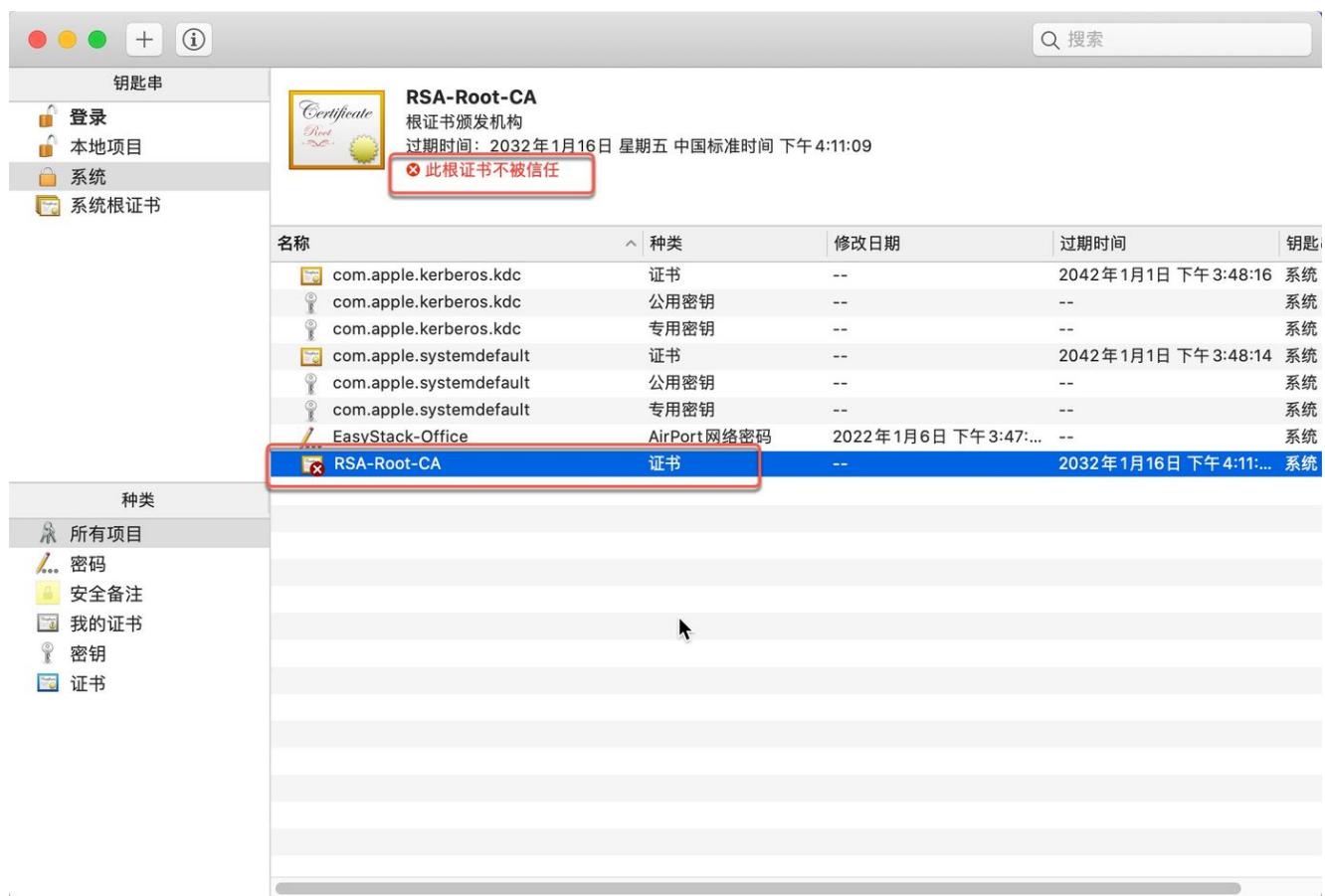
1. 在证书服务页面，下载该私有证书的签发CA链上所有的CA证书文件，即该证书的签发CA、签发CA的上一级签发CA，以此类推直至根CA。
2. 双击某个证书文件，弹出密码输入窗口。



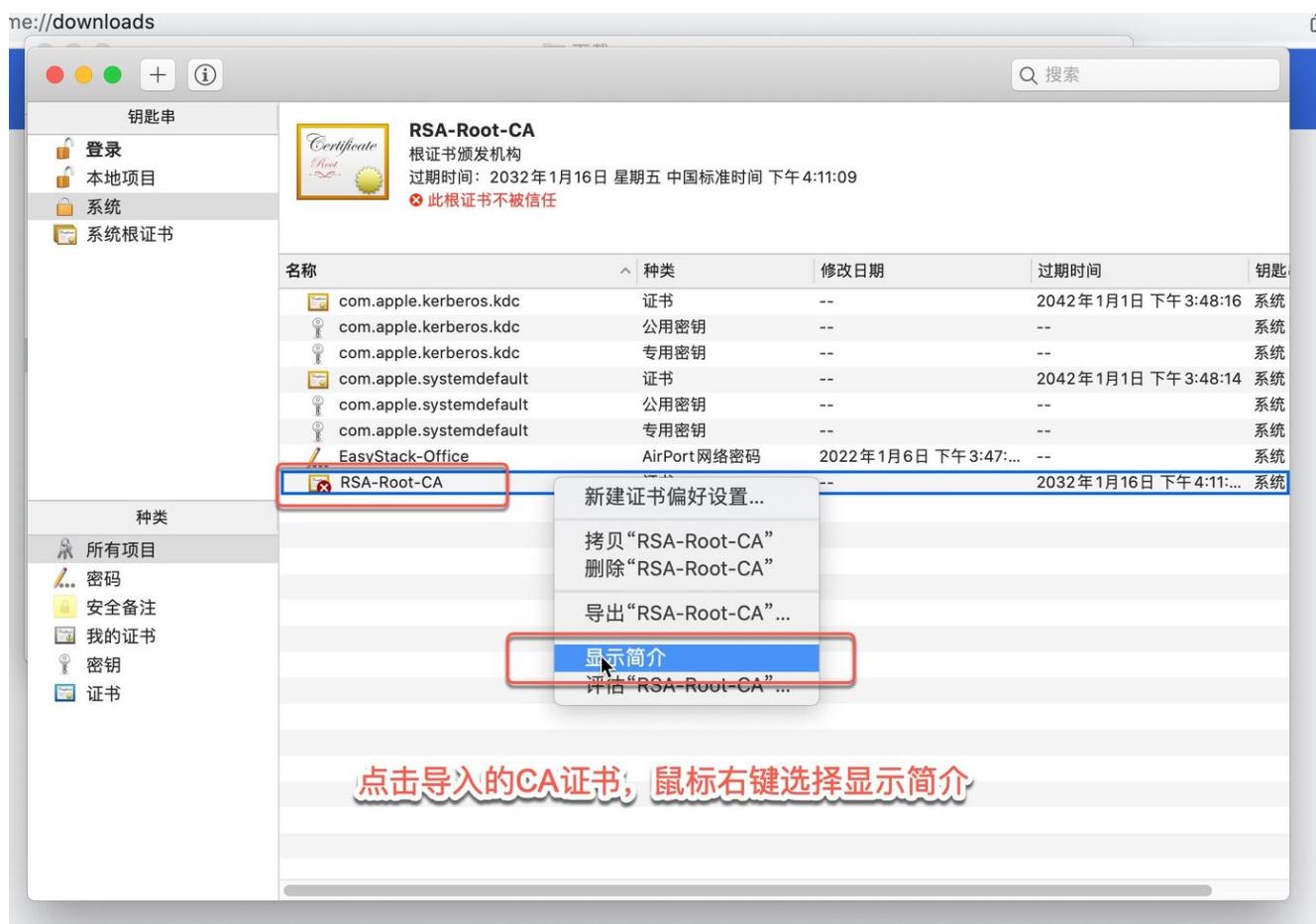
3. 输入系统密码，单击 **修改钥匙串**，弹出钥匙串列表。



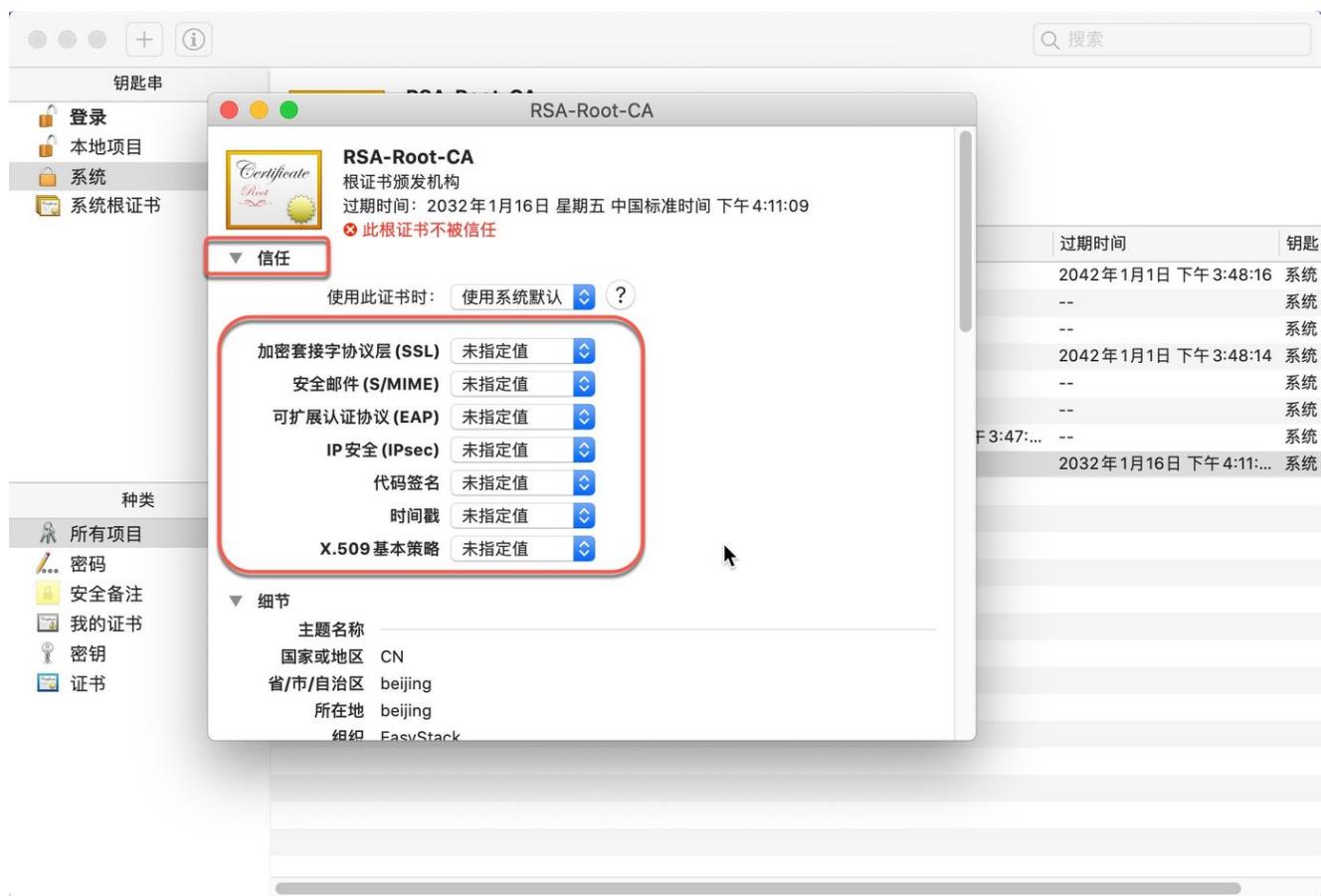
4. 此时虽然私有CA的证书已经导入到系统钥匙串中，但仍不受系统信任。



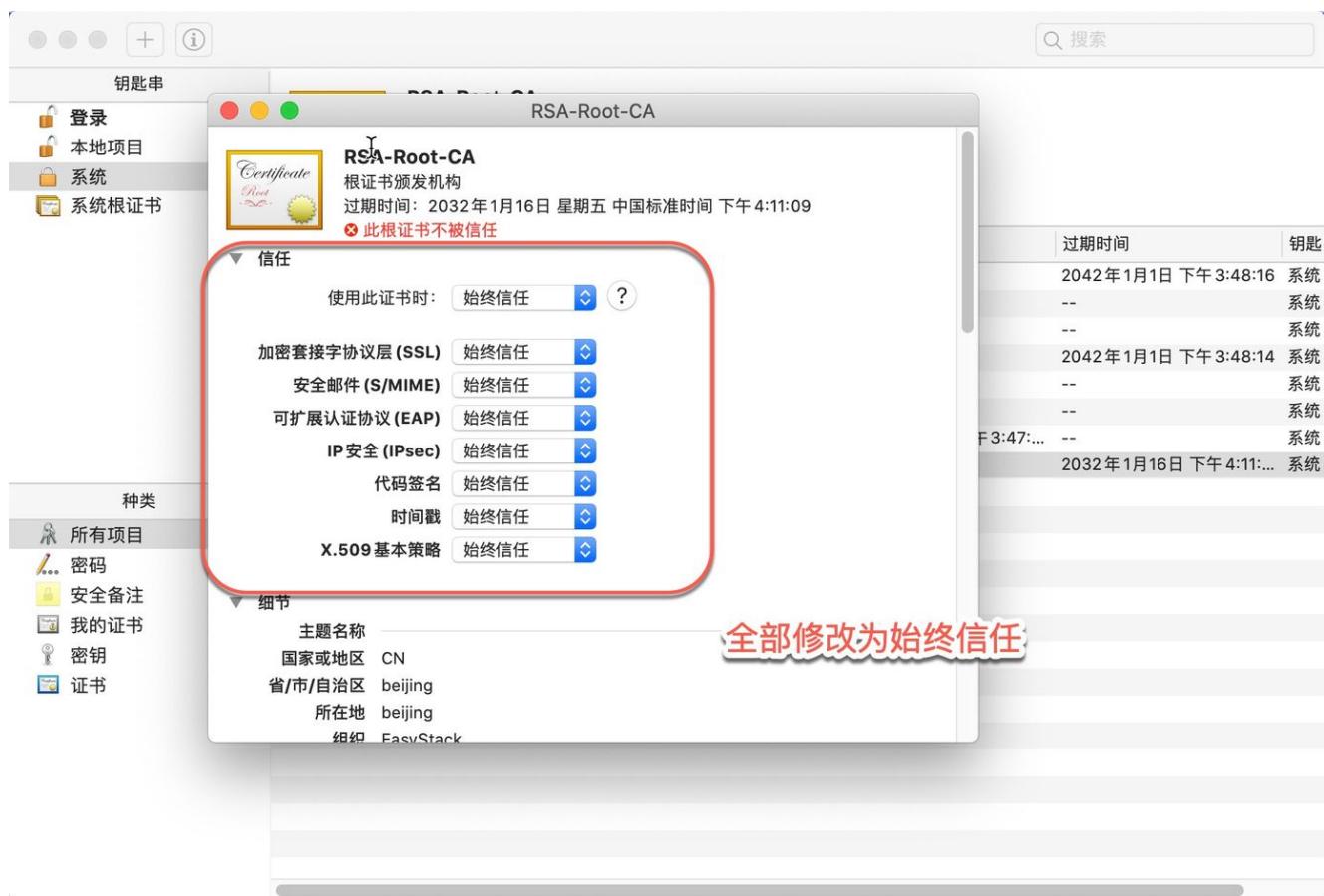
5. 右键单击导入的私有CA证书，选择“显示简介”。



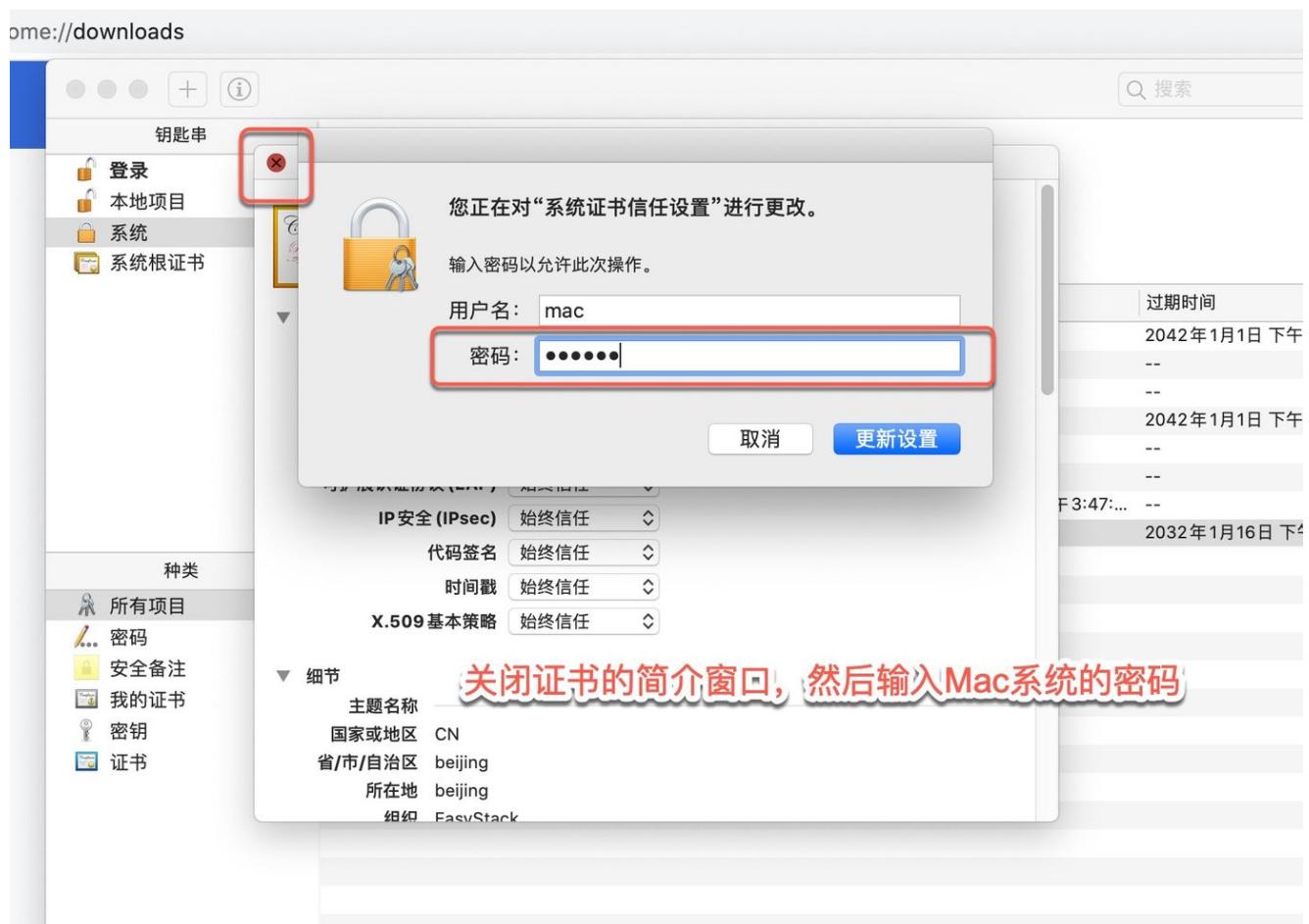
6. 展开“信任”下的详细信息。



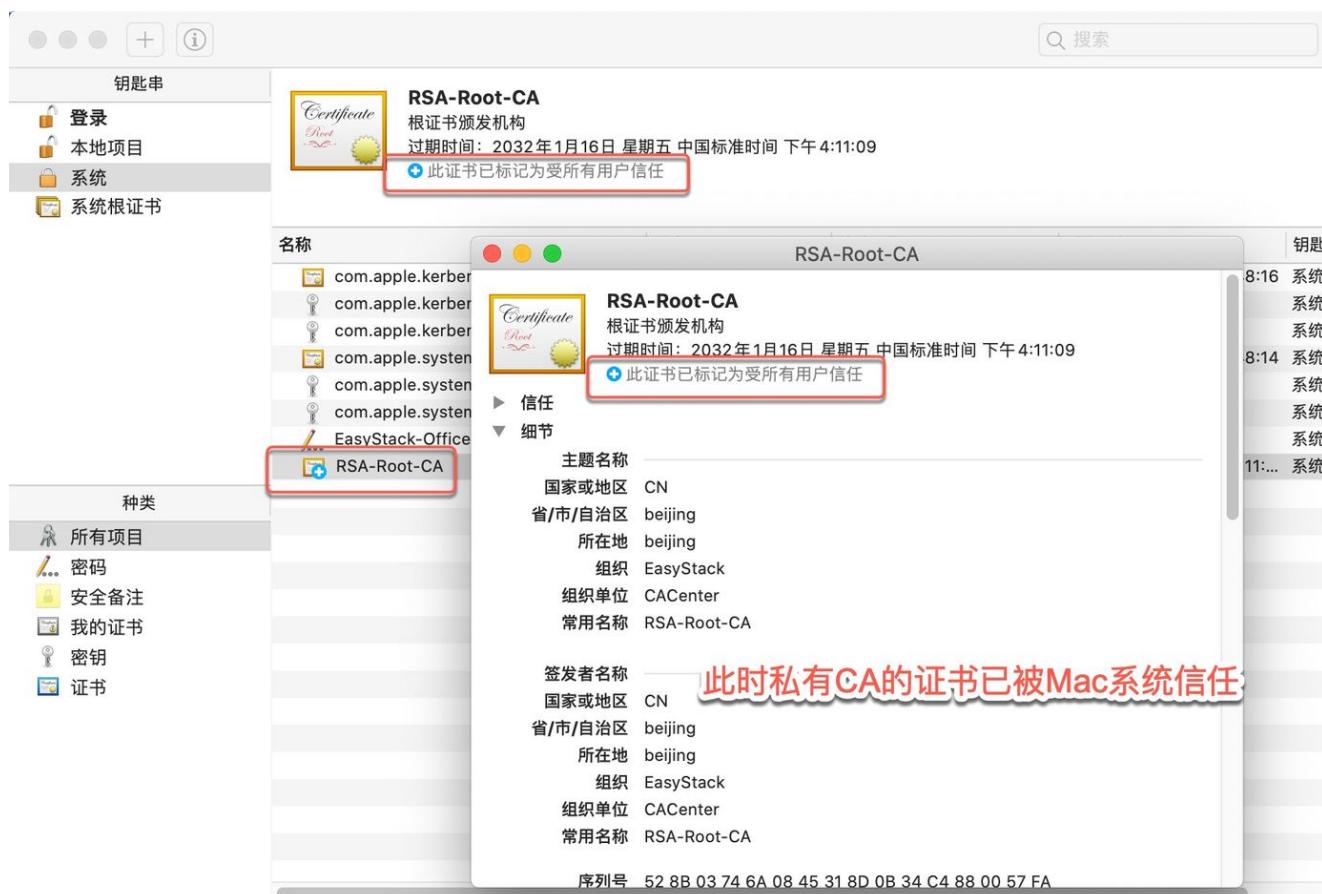
7. 将详细信息中的所有选项改为“始终信任”。



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**。



The screenshot shows the Firefox privacy settings page (`about:preferences#privacy`). The 'Privacy & Security' section is highlighted with a red border. Other sections like '常规' (General), '主页' (Home), '搜索' (Search), and '同步' (Sync) are visible but not selected.

**隐私与安全**

**欺诈内容和危险软件防护**

拦截危险与诈骗内容(B) [详细了解](#)

拦截危险的下载项(D) [详细了解](#)

发现流氓软件或罕见软件时发出警告(C) [详细了解](#)

**证书**

查询 OCSP 响应服务器, 以确认证书当前是否有效(Q) [详细了解](#)

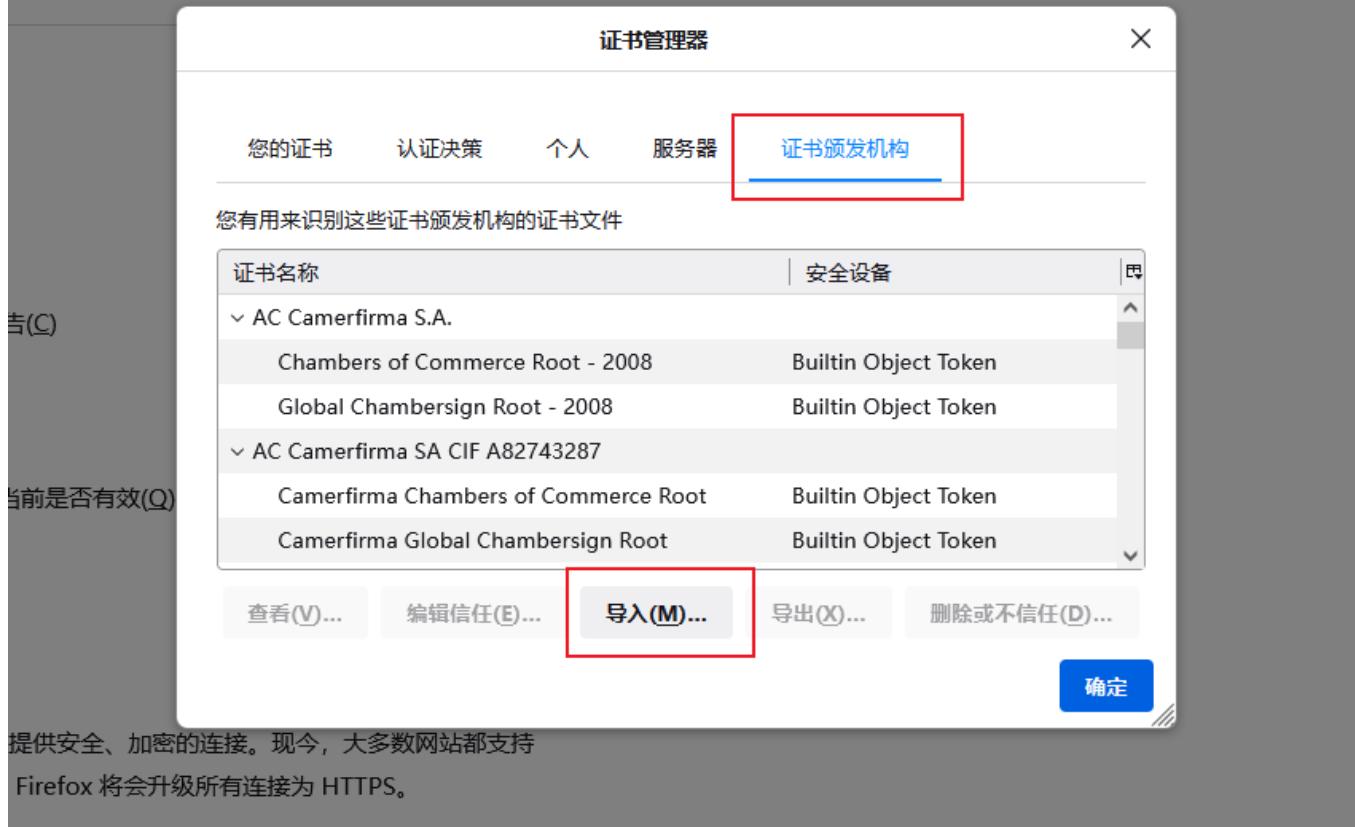
[查看证书...\(C\)](#)

[安全设备...\(D\)](#)

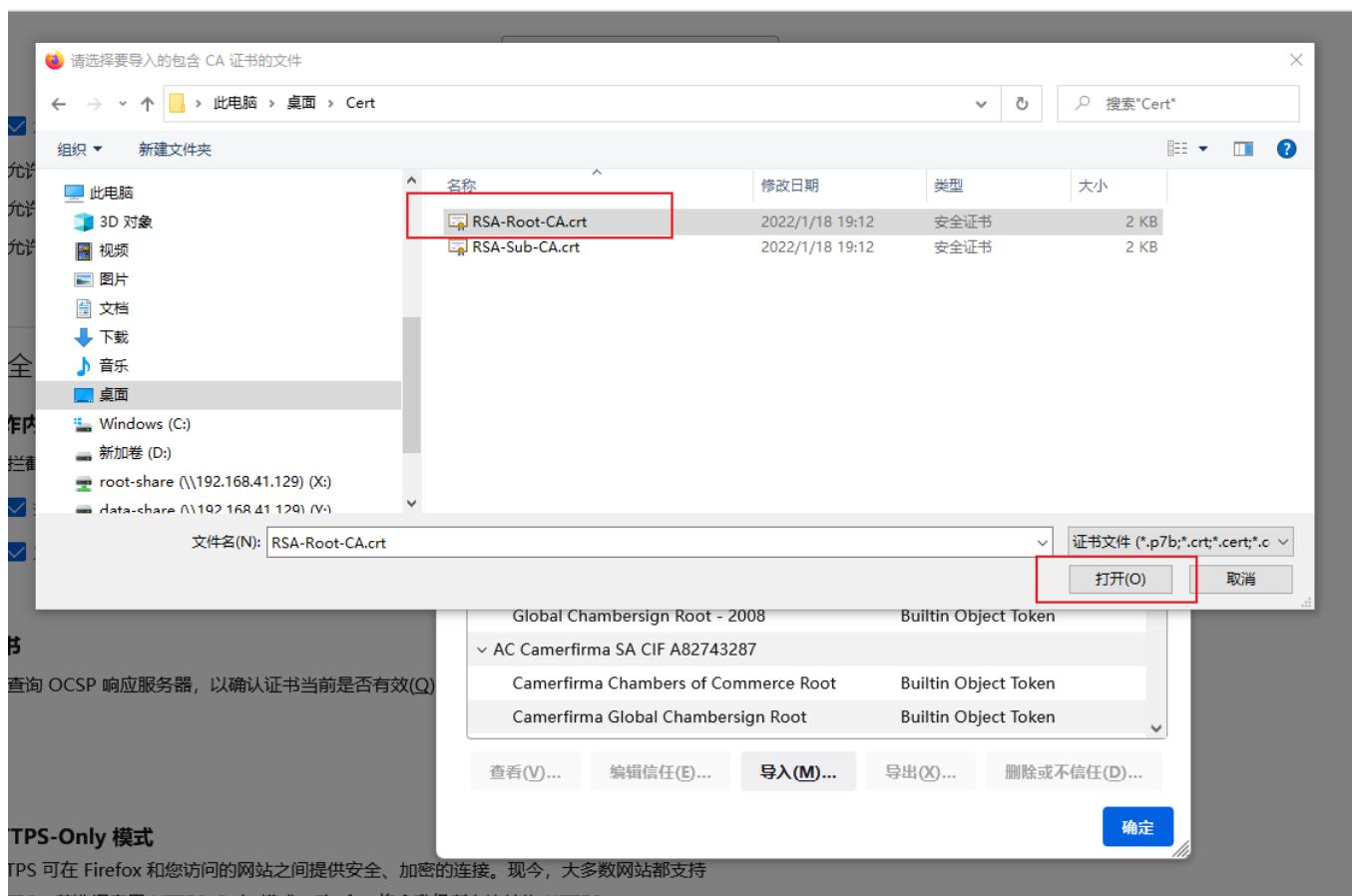
#### HTTPS-Only 模式

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](#)。

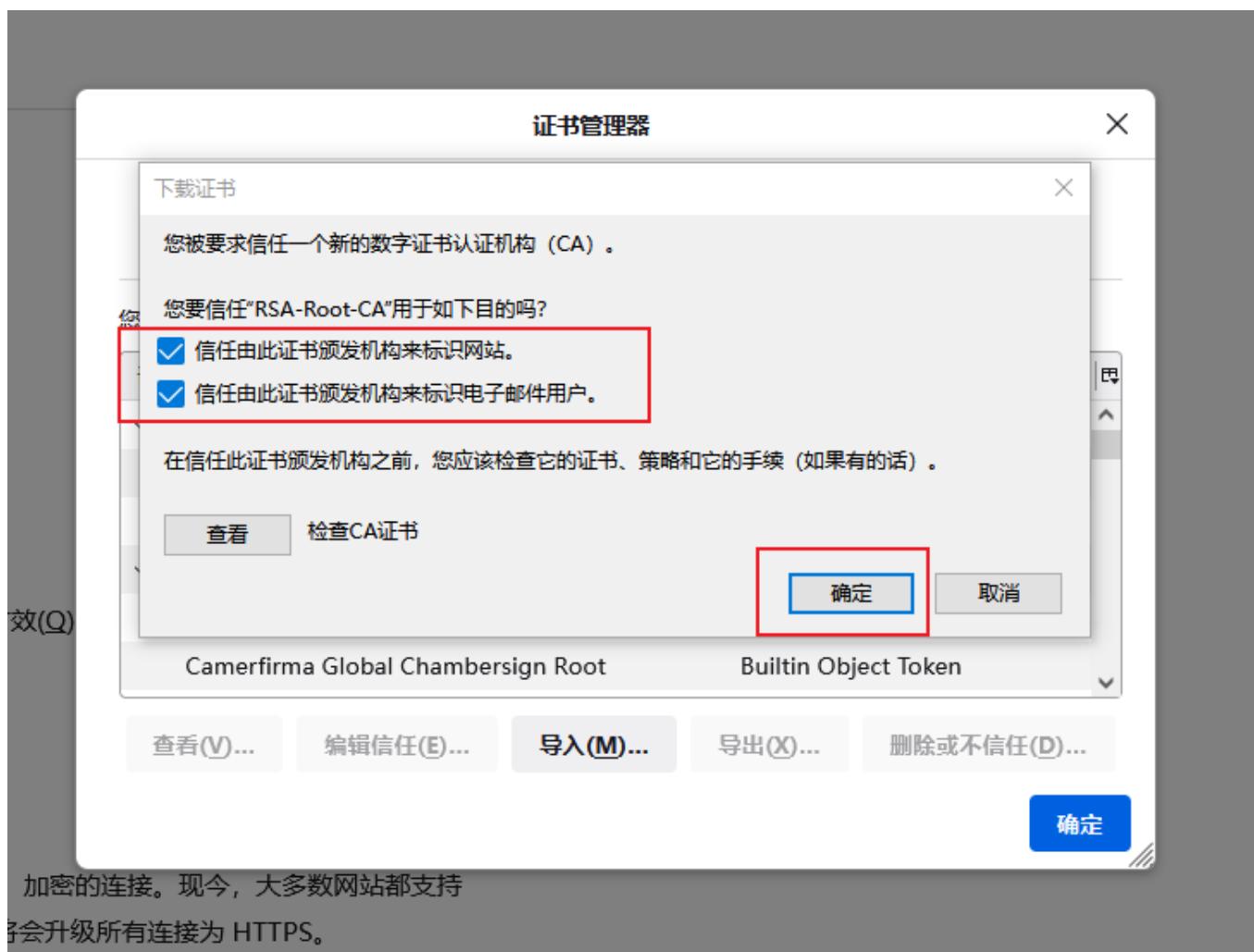
展使用报告，帮助进一步改进用户体验(U) [详细了解](#)



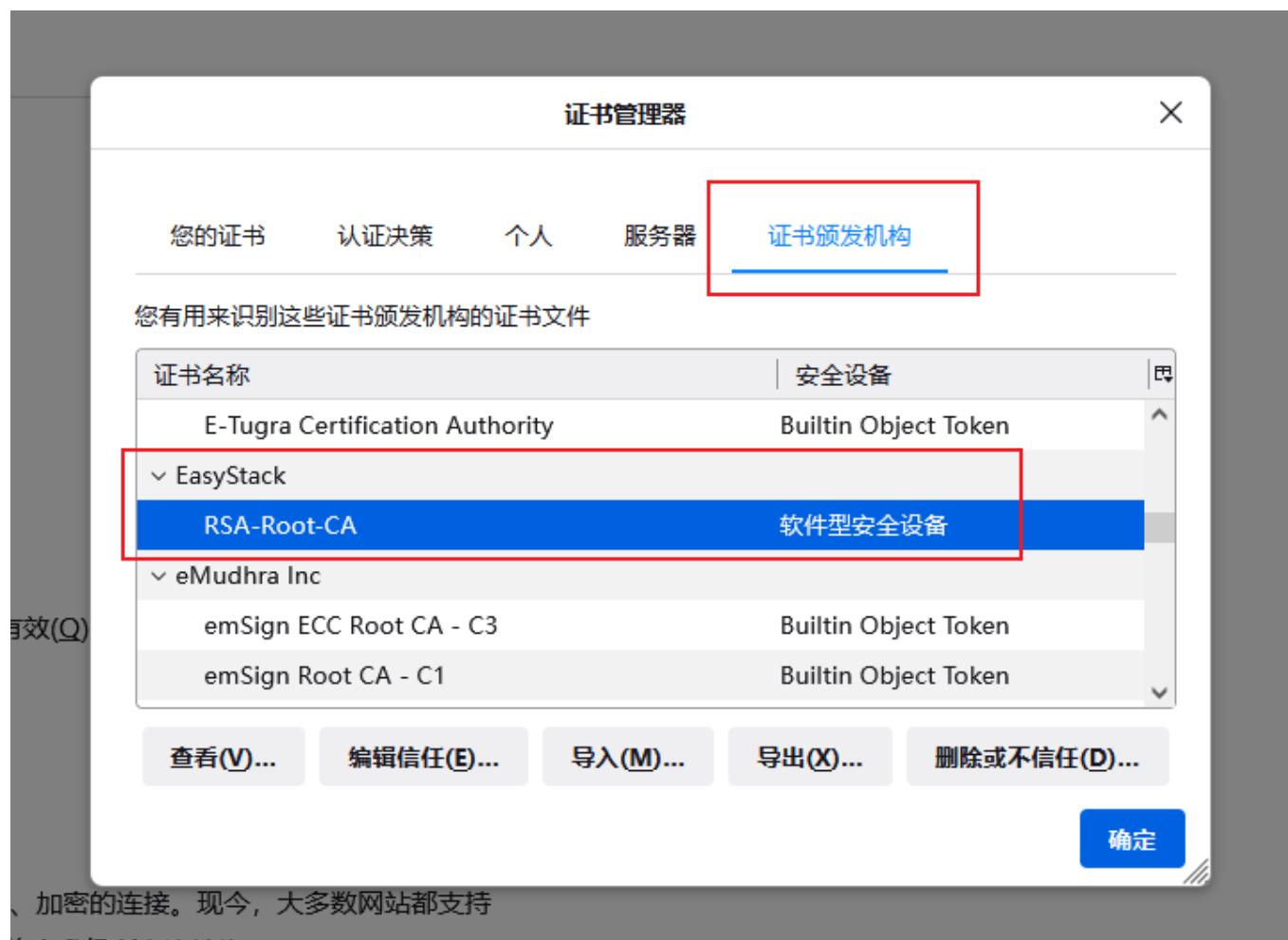
5. 选择下载好的私有CA证书文件，单击 [打开](#)。



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 。



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](mailto:contact@easystack.cn) (业务咨询)

[partners@easystack.cn](mailto:partners@easystack.cn) (合作伙伴咨询)

[marketing@easystack.cn](mailto:marketing@easystack.cn) (市场合作)

[training@easystack.cn](mailto:training@easystack.cn) (培训咨询)

[hr@easystack.cn](mailto:hr@easystack.cn) (招聘咨询)