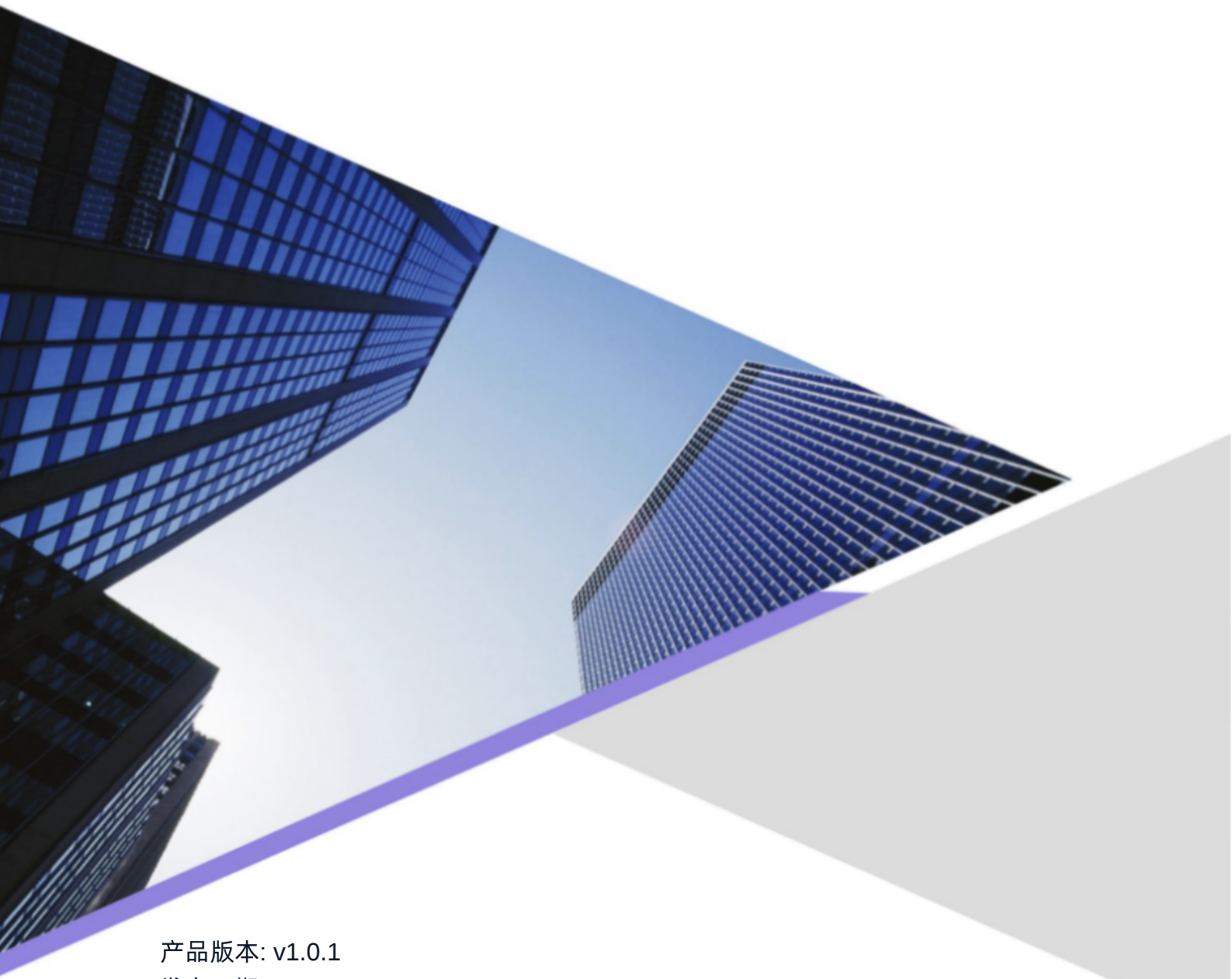
EasyStack
易捷行云

证书服务

使用手册



产品版本: v1.0.1

发布日期: 2024-06-05

目录

1 版本说明

1.1 版本说明书

版本信息

产品名称	产品版本	发布日期
证书服务	V1.0.1	2022-01-21

更新说明

新增功能

- 支持私有CA的全生命周期管理。
- 支持私有CA签发证书，证书的全生命周期管理。
- 支持RSA2048、RSA4096、ECC256、ECC384多种密钥算法。
- 支持国密SM2密钥算法和SM3签名哈希算法生成双证书。
- 支持X.509 v3证书格式，符合PKI/CA国际标准。

依赖说明

> - 安装本产品前需确保平台版本为6.0.2。

2 产品介绍

2.1 什么是证书服务

证书服务是平台上提供私有CA及数字证书全生命周期管理的服务，帮助企业搭建和维护自己的CA体系，包括根及多级中间CA，同时，支持在企业内部签发和管理私有证书，以及托管企业购买的或第三方生成的证书。证书管理服务帮助企业无需花费高昂费用即可实现企业内部的应用身份认证和数据加解密，从而识别和保护组织内的应用程序、服务、设备和用户等资源。

产品优势

- **证书全生命周期管理**

  证书可以通过简单的可视化操作建立完整的CA层次体系，包括根及多级中间CA等，通过CA签发证书，支持对CA和证书的完整生命周期管理。

- **多种密钥算法**

  证书支持RSA2048、RSA4096、ECC256、ECC384等多种密钥算法，支持X.509 v3证书格式，符合PKI/CA国际标准，支持国密算法，包括：国密SM2密钥算法和SM3哈希签名算法。

- **证书托管**

  可以将本地的证书上传到证书服务，实现用户对证书的统一管理。

- **与云产品无缝集成**

  与独享型负载均衡服务深度集成，当负载均衡监听器使用HTTPS服务时支持选择可用的证书，提供统一交互体验。

- **资源成本低**

  证书避免高昂的商业证书开销，尤其开发、测试阶段使用免费证书就可以测试商业证书的功能，大幅降低IT成本。

- **兼容性保证**

兼容主流浏览器和主流操作系统。兼容国际/国内主流算法，RSA/ECC/SM等系列算法。

硬件密码机符合国家密码局认证或FIPS 140-2第3等级认证，能对高安全性要求的用户提供高性能专属加密服务，保障数据安全，规避风险。

主要功能

私有CA管理

私有CA分为根CA和从属CA，根CA下可以包含多个从属CA，每个从属CA下可以包含多个下一级的从属CA，从而形成一套CA层次结构。但对于每套CA层次结构，只有最顶层的CA被称为根CA。本产品支持的CA层级最多可达8级，同时支持CA的启动/禁用、删除等生命周期管理操作。

证书管理

- **证书生命周期管理**

  支持创建、查看、编辑、下载、删除证书。支持多种密钥算法，包括RSA2048、RSA4096、ECC256、ECC384、国密SM2。证书文件格式适配多种服务器类型，例如Tomcat、Nginx、Apache、IIS。

- **第三方证书托管**

  支持上传第三方生成的证书，实现统一管理。

2.2 证书使用场景

- **平台中的云产品使用**

  在证书服务中创建的证书，可在本平台中其它云产品中直接使用，例如在其它云产品创建资源过程中直接选择已创建的证书（具体方式由对应云产品决定）。

- **企业内网应用使用**

  可用于企业内部应用数据需要密码技术提供加密的场景。这种场景需要将创建好的证书下载使用。

2.3 基本概念

本小节将介绍一些与数字证书相关的通用技术名词或原理。若已熟悉相关技术，可忽略本节内容；若尚不熟悉或对其中某部分不了解，可以阅读本小节进行了解。您也可以查阅更多专业资料以便深入了解。

加密与密钥

加密是保证数据传输安全性的一种手段，即使用密钥对明文数据进行加密处理，使其成为不可读的密文，密文通过密钥解密后可还原出明文。按照加解密使用的密钥是否相同，相同的称为对称加密，不同的称为非对称加密。数字证书的工作原理即为非对称加密。非对称加密使用到的两个不同的密钥通常被称为“公钥”和“私钥”。公钥加密的数据只能用私钥解密，同理，私钥加密的数据只能用公钥解密。私钥只能由使用者拥有与使用，不可泄漏，公钥可以公开给所有人。在本平台创建私有证书时系统会自动生成证书文件和私钥文件，对应的公钥即保存在证书文件中。

数字签名与数字证书

在数据收发过程中，若要保证数据安全，需要考虑两个问题：如何证明发送内容没有被篡改、如何证明内容确实来自真正想要通信的对方。

第一个问题，为了保证传输的数据内容不被篡改，发送数据方需要基于数据计算出一个“指纹”，并将“指纹”与数据一同发送出去。这个“指纹”其实是使用哈希算法计算出内容的哈希值，这个哈希值是唯一的，且无法通过哈希值推导出内容。接受数据方收到消息后，也基于数据计算出一个“指纹”，并与发送者发来的指纹进行比对。如果一致则认为内容没有被篡改，如果不一致则证明内容可能被篡改过。

在这个过程中，虽然确保了内容没有被篡改过，但是无法保证“内容+哈希值”整体没有被人替换过，于是还需要考虑第二个问题，保证没有篡改过的数据确实来自真正想要通信的对方。

确认身份的第一种手段就是 数字签名，即发送方使用私钥对“指纹”进行加密。同时发送方需要公布自己的公钥。这样接收方如果能用该公钥解密，就说明消息是由持有私钥的人发的。但如果有恶意者伪造了公钥，恶意者拿着自己的公钥和私钥仍然可以冒充发送方与接收方通信，因此还需要引入一个第三方权威机构来证明公钥确实是来自发送方的。

发送方将自己的公钥与身份信息发送给CA（数字证书认证机构），CA使用自己的私钥对发送方的公钥和身份信息等内容进行数字签名，并把“身份等信息+公钥+数字签名”打包成一个 数字证书。通信过程中发送方向接收方展示自己的数字证书，接收方使用CA的公钥（通常浏览器和操作系统中集成了权威CA的公钥）解密证书

中的数字签名得到哈希值，再与计算出的哈希值对比，若一致则证明公钥确实来自真正的发送方而非恶意者冒充。此时接收方可以使用保存在证书中的发送方的公钥进行后续的通信。

至此，即可保证收到的数据确实来自正确的发送方且未被篡改过。

通常，向互联网上认可的权威CA机构申请证书是需要高昂费用的，因此有时需要使用私有证书，私有证书虽然在互联网上不受信任，但是可满足企业内部应用数据需要密码技术提供加密的需求。

数字证书与HTTPS

HTTPS是一种基于SSL协议的网站加密传输协议，网站安装数字证书后，可以使用HTTPS加密协议访问，实现了客户端与服务端之间的加密通信通道，防止传输数据被泄露或篡改。简单来说，HTTPS是HTTP的安全加强版，而想要使用HTTPS，则需先安装数字证书。

2.4 产品获取

1. 获取并安装“证书服务”云产品。

   在顶部导航栏中，依次选择[产品与服务]-[产品与服务管理]-[云产品]，进入“云产品”页面获取并安装“证书服务”云产品。具体操作说明，请参考“产品与服务管理”帮助中“云产品”的相关内容。

2. 访问证书服务。

   在顶部导航栏中，依次选择[产品与服务]-[证书服务]，选择各子菜单，即可访问对应服务。

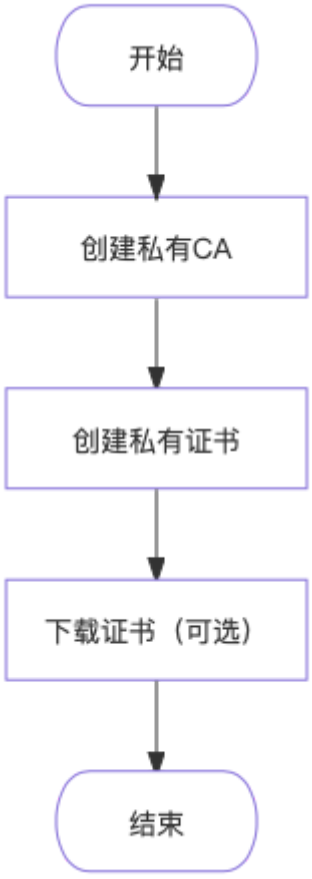
2.5 权限说明

* 云管理员可以管理平台中所有私有CA及证书，其他用户仅能管理自己所在项目的私有CA及证书。

3 快速入门

3.1 操作指引

证书管理服务云产品的主线使用流程及具体说明如下：



操作流程	描述
创建私有CA	创建证书时需选择由哪个私有CA签发。若所需私有CA已存在，可跳过此步直接创建证书。
创建私有证书	确认签发CA存在后，即可创建私有证书。

操作流程	描述
下载证书（可选）	证书创建完成后，可根据证书使用场景选择是否下载证书分发给用户安装使用。

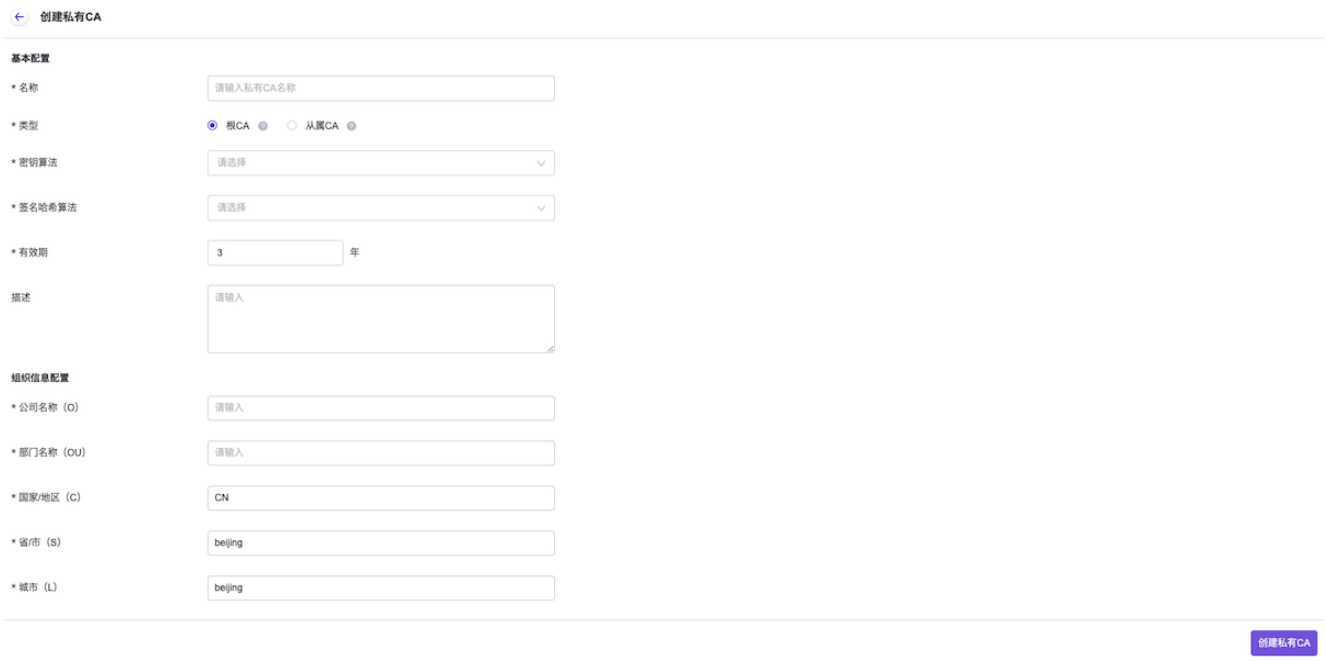
3.2 创建私有CA

> 说明：
> - 项目中首次创建私有CA时只能创建根CA。后续可选择创建根CA或从属CA。
> - 私有CA创建完成后默认为“已启用”状态。

1. 在顶部导航栏中，依次选择[产品与服务]-[证书服务]-[私有CA]，跳转至“私有CA”页面。

2. 单击 `创建私有CA` ，跳转至“创建私有CA”页面。

3. 配置参数。



参数	说明
类型	私有CA分为根CA和从属CA，根CA下可以包含多个从属CA，每个从属CA下可以包含多个下一级的从属CA，从而形成一套CA层次结构。但对于每套CA层次结构，只有最顶层的CA被称为根CA。因此，若要建立新的CA层次结构，可选择“根CA”；若要在现有CA层次结构中增加新的成员，可选择“从属CA”。
签发CA	仅当“类型”选择“从属CA”时显示，选择该从属CA由哪一私有CA签发。

参数	说明
密钥算法	选择私有CA签发证书时所使用的加密算法类型。当前支持RSA2048、RSA4096、ECC256、ECC384、国密SM2。对于从属CA，若其签发CA使用的是国密SM2算法，则从属CA只能使用相同算法。
签名哈希算法	选择私有CA签发证书时所使用的哈希算法类型。当前支持SHA256、SHA384、SHA512、国密SM3。当且仅当“密钥算法”参数选择了“国密SM2”时，本参数可选择“国密SM3”。
有效期	根CA有效期的取值范围为3至30年。从属CA有效期的取值范围为1至20年，同时，不能超过其签发CA的剩余有效期。有效期不足1年时，无法签发从属CA。有效期结束后私有CA将变为“已过期”状态，无法继续签发证书，且该私有CA曾经签发过的证书也将失效。
路径深度	路径深度决定了该CA可以继续签发下级从属CA的层级，可填写的最小值为0，最大值=其签发CA的路径深度-1。签发CA的路径深度可在其详情页的“基本信息”区域查看。根CA的默认路径深度为7。路径深度为0的私有CA无法继续签发从属CA（签发私有证书不受影响）。例如，某一根CA名称为a，现创建一个由a直接签发的从属CA，名称为b，则b的路径深度可设置的范围为0～6（左右包含）中的整数。假设b的路径深度设置为6，则由b签发的证书链中深度最大的一条可能的情况是：b->c->d->e->f->g->h。
公司名称	根据申请单位实际情况填写即可。
部门名称	
国家/地区	
省/市	
城市	

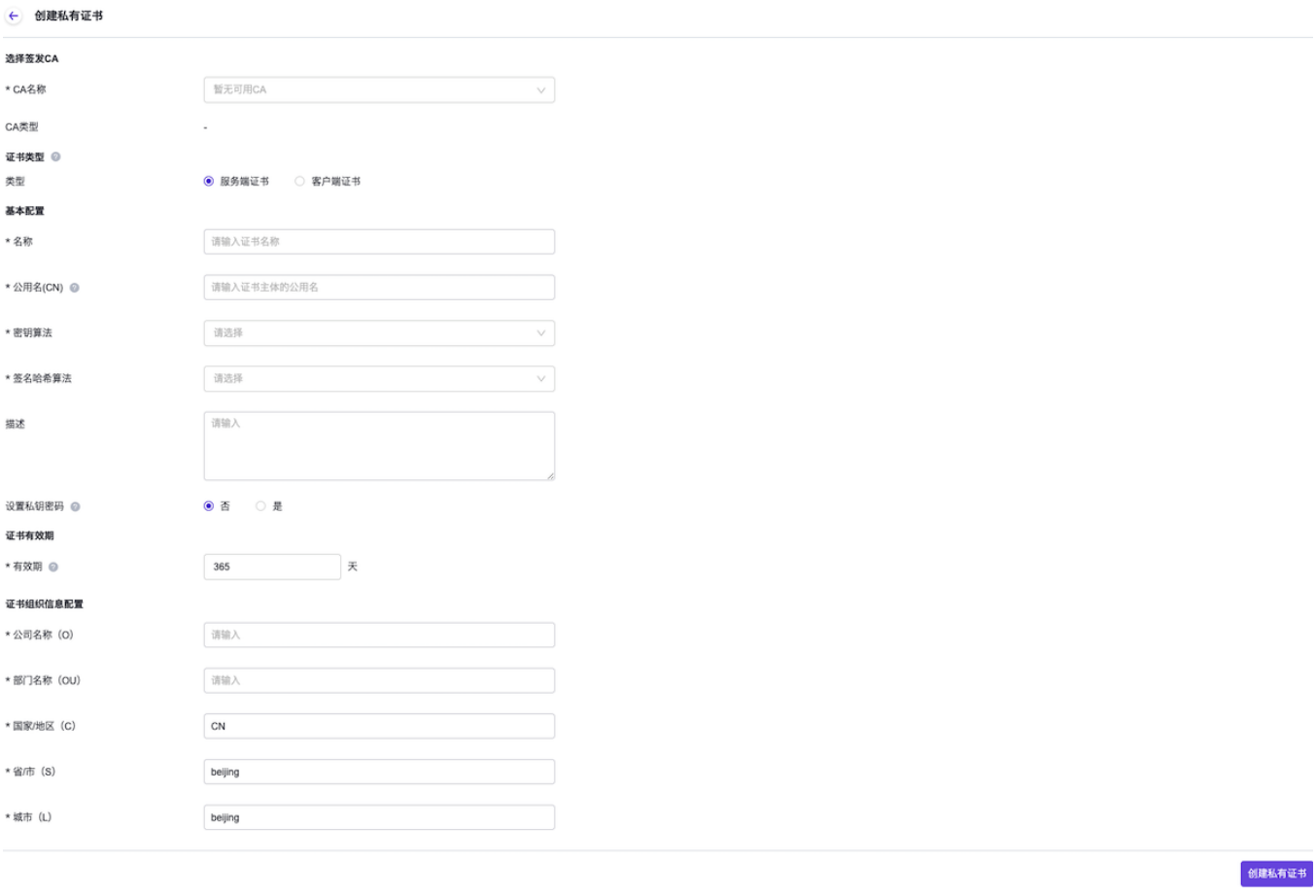
4. 单击 `创建私有CA` ，完成操作。

3.3 创建私有证书

创建证书时将自动生成证书文件及私钥。

> 说明：
> 创建完成后，除描述外其它信息均不支持修改。

1. 在顶部导航栏中，依次选择[产品与服务]-[证书服务]-[证书管理]，进入“证书管理”页面。
2. 单击 `创建私有证书` ，跳转至“创建私有证书”页面。
3. 配置参数，单击 `创建私有证书` 完成操作。



参数		说明
选择签发CA	CA名称（CN）	选择签发该证书的CA。

参数		说明
	类型	签发该证书的CA的类型，包括根CA和从属CA，根据所选CA自动显示，无需配置。
证书类型	类型	证书类型分为服务端证书和客户端证书。服务端证书安装到应用的服务器端，用于证明站点所有者身份；客户端证书安装到访问应用的客户端软件，用于验证客户端身份。
基本配置	名称	私有证书的名称。
	公用名（CN）	私有证书主体的通用名称。 * 服务端证书通常填写服务域名，如果未指定域名，那么在使用生成的服务端证书配置HTTPS服务后，浏览器访问服务时可能提示“此站点不安全”等。域名支持以“*”开头的泛域名。 * 客户端证书通常填写用户邮箱地址或者用户名等可以标识客户端身份的信息。
	密钥算法	证书使用的密钥算法和密钥的位大小，当前支持RSA2048、RSA4096、EC256、EC384、国密SM2。若签发CA使用的密钥算法为“国密SM2”，则本参数只能使用相同算法。若签发CA使用的密钥算法非“国密SM2”，则本参数不支持选择“国密SM2”。
	签名哈希算法	证书使用的签名哈希算法，当前支持SHA256、SHA384、SHA512、国密SM3。当且仅当“密钥算法”参数选择了“国密SM2”时，本参数可选择“国密SM3”。
	设置私钥密码	私钥密码用于对证书私钥进行加密，目前不支持密码找回功能，请牢记私钥密码，后续安装私有证书时，需要使用此处密码对私钥解密。
证书有效期	有效期	证书有效期应小于其签发CA的剩余有效期，且上限为7300天。若签发CA剩余有效期不足1天，则无法签发证书。有效期结束证书即失效，访问使用该证书的应用时，将提示证书已过期。
证书组织信息配置	公司名称	根据证书隶属组织实际情况填写即可。
	部门名称	

参数		说明
	国家/地区	
	省/市	
	城市	

3.4 下载证书

下载证书分发给用户安装使用。

1. 在顶部导航栏选择[产品与服务]-[证书服务]-[证书管理]，进入“证书管理”页面。

2. 单击目标证书操作栏的 `下载` ，弹出“下载证书”对话框。

3. 不同密钥算法的证书下载方式及文件格式如下：

   - 使用RSA和ECC密钥算法的证书：选择服务器类型，单击 `下载` 完成操作。
   - 使用国密算法的证书：直接单击 `下载` 完成操作。国密证书目前仅支持下载通用格式的证书文件，包含签名证书和加密证书双证书，详细说明见下方表格。

使用RSA和ECC密钥算法的证书文件说明：

证书类型	服务器类型	证书压缩包中的文件	文件说明
服务端证书	Tomcat	server.jks	Java KeyStore格式的证书文件。
		keystorePass.txt	加密证书的密码。
	Nginx	server.crt	证书文件。
		server.key	证书对应的私钥文件。
		chain.crt	该证书的签发CA到根CA的CA证书链文件。
	Apache	server.crt	证书文件。
		server.key	证书对应的私钥文件。
		chain.crt	该证书的签发CA到根CA的CA证书链文件。
	IIS	server.pfx	PKCS#12格式的证书文件。

证书类型	服务器类型	证书压缩包中的文件	文件说明
		keystorePass.txt	加密证书的密码。
	其他	server.pem	证书文件。
		server.key	证书对应的私钥文件。
		chain.pem	该证书的签发CA到根CA的CA证书链文件。
客户端证书	Tomcat	client.crt	证书文件，按需配置到客户端中即可。
		client.key	证书对应的私钥文件，按需配置到客户端中即可。
		client.pfx	证书和私钥合并后的PKCS#12证书文件(证书未加密)，按需配置到客户端中即可。使用合并的证书文件与使用单独的证书&私钥文件两种方式二选一即可。
		client- ca.truststore	证书签发CA的Truststore文件，需配置到Tomcat服务配置文件中的 **truststoreFile** 处。
		keystorePass.txt	加密client-ca.truststore文件的密码，需配置到Tomcat服务配置文件中的 **truststorePass** 处。
	Nginx	client.crt	证书文件，按需配置到客户端中即可。
		client.key	证书对应的私钥文件，按需配置到客户端中即可。
		client.pfx	证书和私钥合并后的PKCS#12证书文件(证书未加密)，按需配置到客户端中即可。使用合并的证书文件与使用单独的证书&私钥文件两种方式二选一即可。

证书类型	服务器类型	证书压缩包中的文件	文件说明
		client-ca.pem	证书的签发CA到根CA的CA证书链文件，需配置到Nginx服务配置文件中 **ssl_client_certificate** 处，并开启 **ssl_verify_client on** 配置。
	Apache	client.crt	证书文件，按需配置到客户端中即可。
		client.key	证书对应的私钥文件，按需配置到客户端中即可。
		client.pfx	证书和私钥合并后的PKCS#12证书文件(证书未加密)，按需配置到客户端中即可。使用合并的证书文件与使用单独的证书&私钥文件两种方式二选一即可。
		client-ca.pem	证书的签发CA到根CA的CA证书链文件，需配置到Apache Httpd服务配置文件中 **SSLCACertificateFile** 处，并开启 **SSLVerifyClient require** 配置。
	IIS	client.crt	证书文件，按需配置到客户端中即可。
		client.key	证书对应的私钥文件，按需配置到客户端中即可。
		client.pfx	证书和私钥合并后的PKCS#12证书文件(证书未加密)，按需配置到客户端中即可。使用合并的证书文件与使用单独的证书&私钥文件两种方式二选一即可。
		client-ca.pem	证书的签发CA到根CA的CA证书链文件，需将证书链文件中的每一个证书导入到部署IIS服务的Windows系统的“受信任的证书颁发机构”当中。
	其他	client.crt	证书文件，按需配置到客户端中即可。

证书类型	服务器类型	证书压缩包中的文件	文件说明
		client.key	证书对应的私钥文件，按需配置到客户端中即可。
		client.pfx	证书和私钥合并后的PKCS#12证书文件(证书未加密)，按需配置到客户端中即可。使用合并的证书文件与使用单独的证书&私钥文件两种方式二选一即可。
		client-ca.pem	证书的签发CA到根CA的CA证书链文件，需配置到指定服务的客户端证书认证配置项中。

使用国密密钥算法的证书文件说明：

证书类型	证书压缩包中的文件	文件说明
服务端证书	server_sig_cert.pem	签名证书
	server_sig_key.pem	签名证书对应的私钥文件
	server_enc_cert.pem	加密证书
	server_enc_key.pem	加密证书对应的私钥文件
	chain.pem	证书的签发CA到根CA的CA证书链文件
客户端证书	client_sig_cert.pem	签名证书
	client_sig_key.pem	签名证书对应的私钥文件
	client_enc_cert.pem	加密证书
	client_enc_key.pem	加密证书对应的私钥文件
	chain.pem	证书的签发CA到根CA的CA证书链文件

4 用户指南

4.1 私有CA

本章节主要介绍在“私有CA”页面中，针对私有CA的一系列运维管理操作，如：查看详情、启用、禁用、删除等。其中，在云平台的顶部导航栏中，依次选择[产品与服务]-[证书服务]-[私有CA]，即可进入“私有CA”页面。

查看私有CA详情

1. 在“私有CA”页面中，单击私有CA名称链接，跳转至私有CA详情页面，即可查看私有CA详情。

启用/禁用私有CA

私有CA创建完成后默认为“已启用”状态，被禁用后将无法签发下级从属CA和私有证书。

1. 在“私有CA”页面中，单击目标私有CA操作栏的 `启用` 或 `禁用` 按钮，弹出操作提示框。
2. 单击 `启用` 或 `禁用` 完成操作。

编辑私有CA

仅支持修改描述信息。

1. 在“私有CA”页面中，单击目标私有CA操作栏的 `更多` - `编辑` 按钮，弹出编辑对话框。
2. 修改信息，单击 `编辑` 完成操作。

删除私有CA

若目标私有CA下仍存在从属CA或私有证书时，将无法直接删除目标CA，当删除其签发的全部证书和所有从属CA后，方可删除目标CA。

1. 在“私有CA”页面中，单击目标私有CA操作栏的 `更多` - `删除` 按钮，弹出删除提示框。
2. 单击 `删除` 完成操作。

4.2 证书管理

本章节主要介绍在“证书管理”页面中，针对证书的一系列运维管理操作，如：查看详情、上传第三方证书、删除证书等。其中，在云平台的顶部导航栏中，依次选择[产品与服务]-[证书服务]-[证书管理]，即可进入“证书管理”页面。

查看证书详情

用于查看证书的有效期、算法、归属项目等详细信息。

1. 在“证书管理”页面中，单击证书名称链接，即可进入证书详情页面查看信息。

上传证书

可将第三方生成的证书上传至平台进行存储及统一管理。暂不支持上传国密算法的证书。

1. 在“证书管理”页面中，单击 `上传证书` ，弹出“上传证书”对话框。
2. 配置证书名称及描述信息，将证书内容、证书链及证书私钥以文件形式上传或直接输入。
3. 单击 `上传` 完成操作。

编辑证书

仅支持修改描述信息。

1. 在“证书管理”页面中，勾选目标证书，单击 `编辑` ，弹出“编辑描述”对话框。
2. 修改描述信息，单击 `保存` 完成操作。

删除证书

1. 在“证书管理”页面中，选择一个或多个待删除的证书，单击 `删除` ，弹出“删除证书”提示框。
2. 单击 `删除` 完成操作。

5 常见问题

5.1 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。

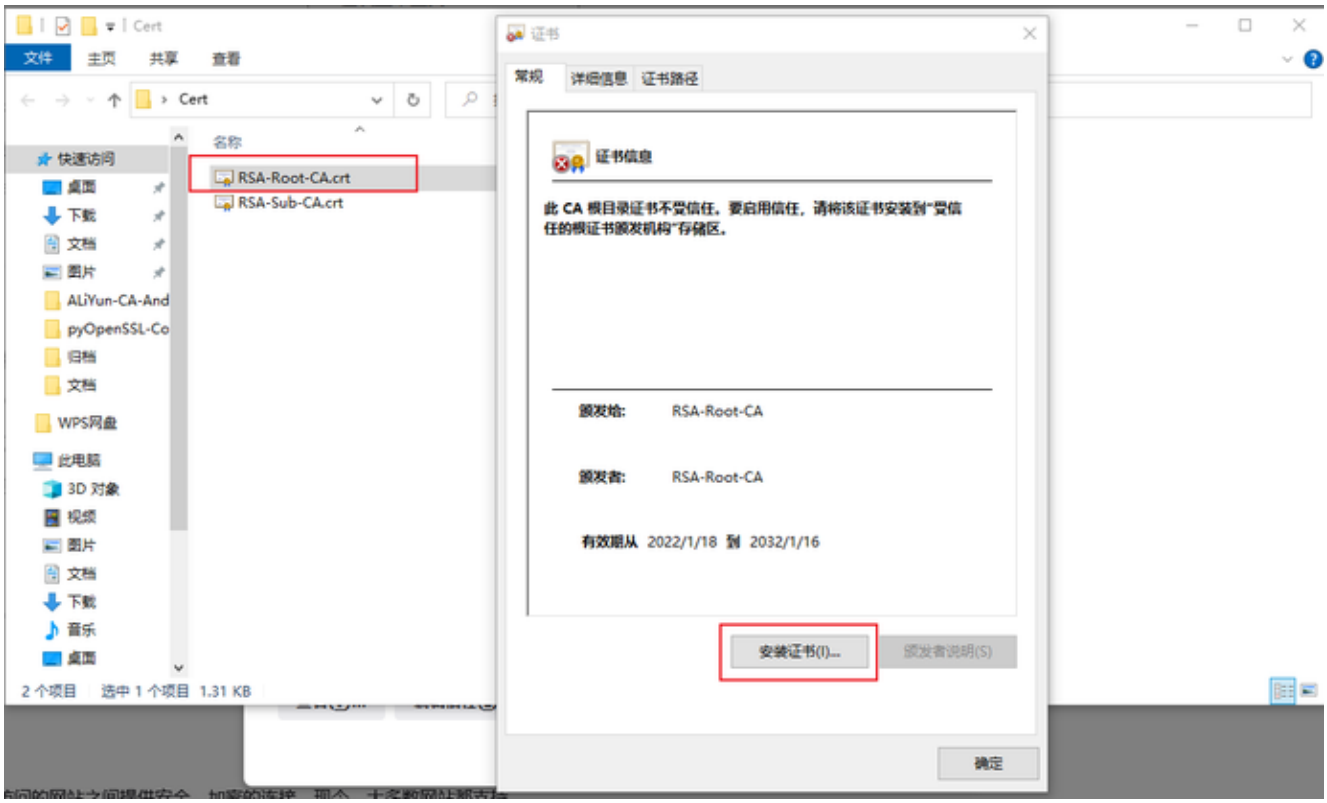
> 说明：
> Firefox浏览器是从浏览器内部的证书库检查当前证书的签发CA是否受浏览器信任，而不是读取操作系统中的证书库，因此其配置方式不同于其它浏览器。

Windows操作系统

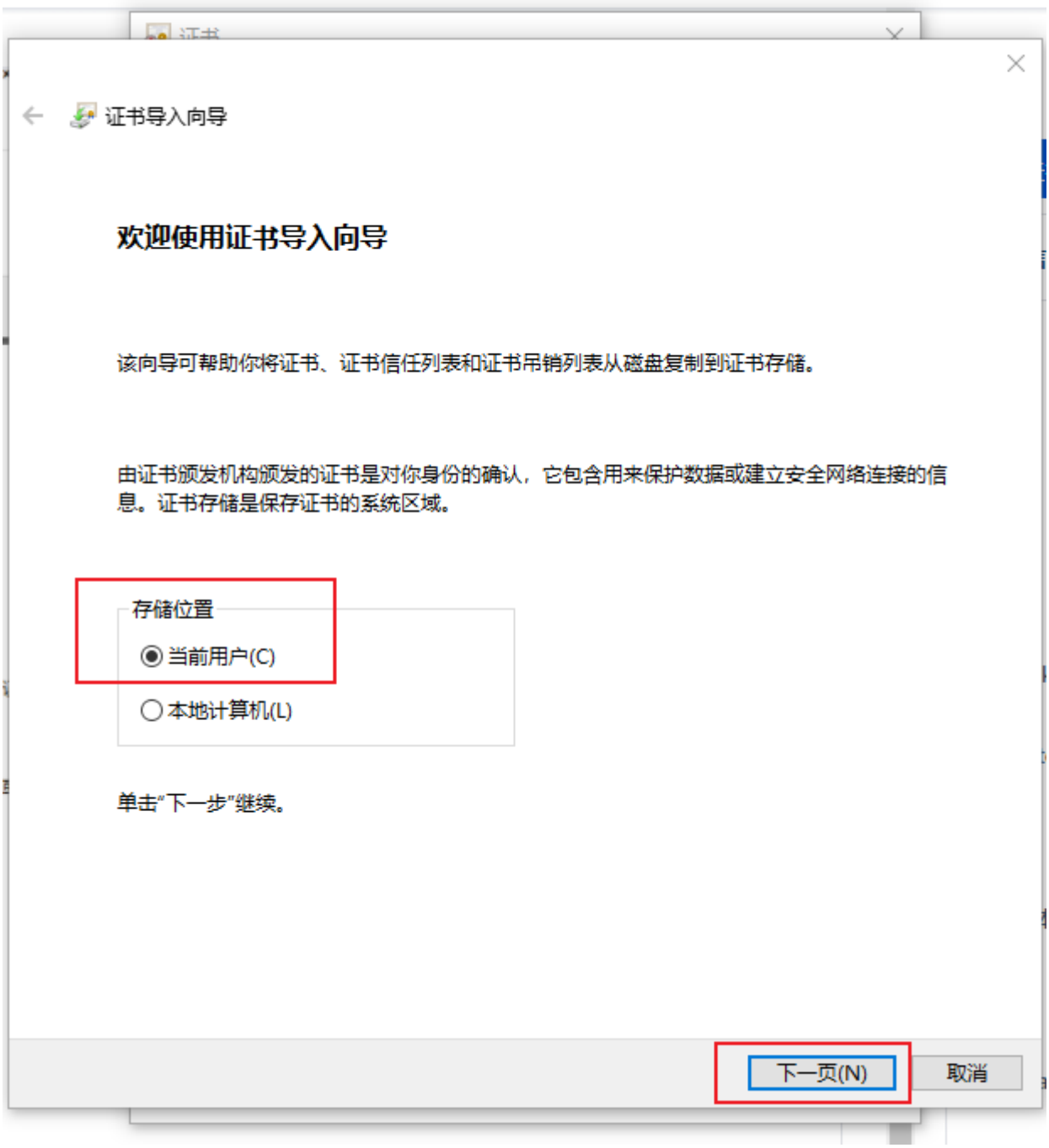
本节介绍在Windows操作系统中，如何导入私有证书的签发CA证书链，使其成为受信任的证书颁发机构。

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。

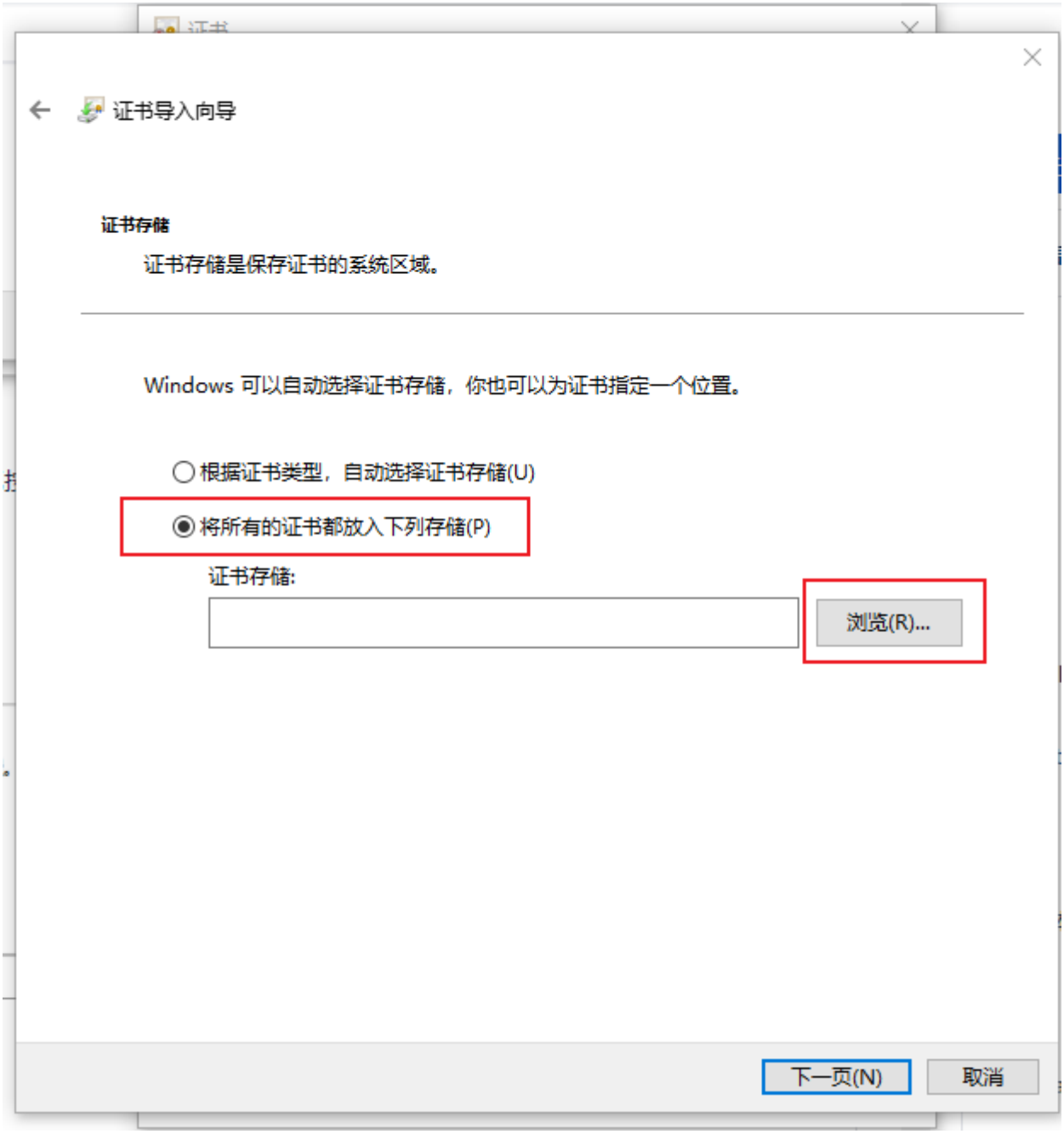
2. 双击某个CA证书文件，在弹出的窗口中单击 `安装证书` 。



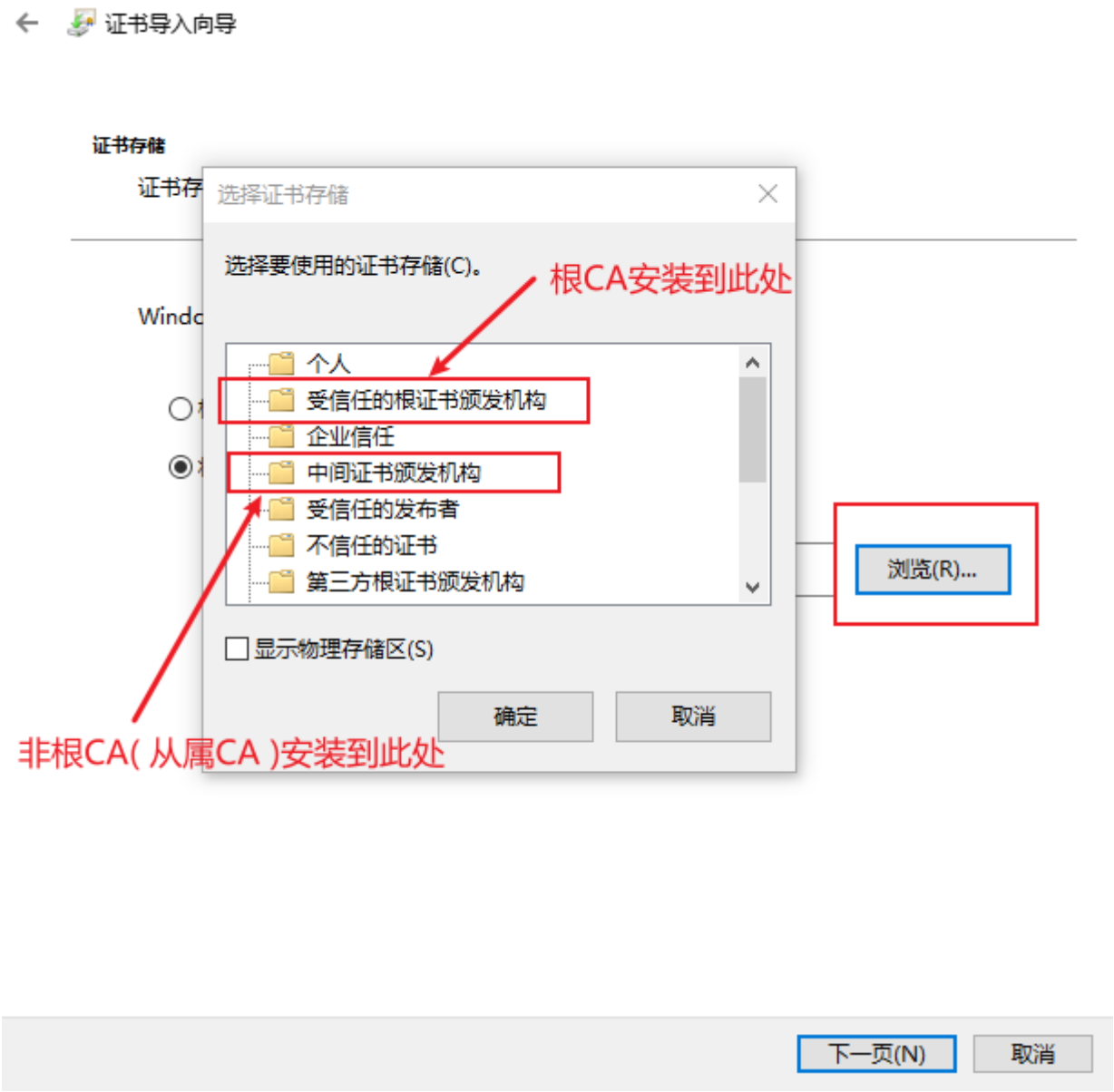
3. 存储位置选择 `当前用户` ，单击 `下一页` 。



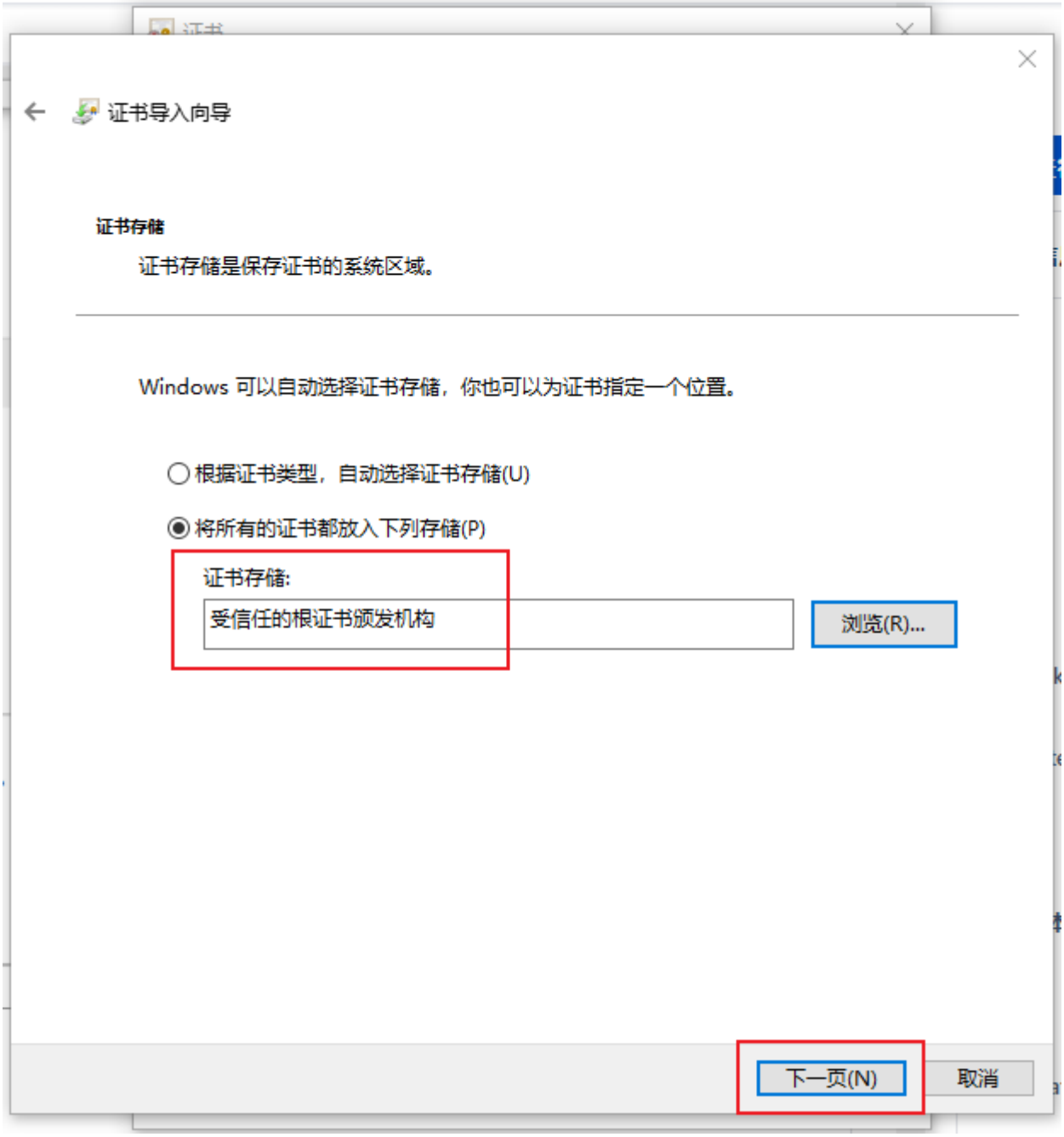
4. 选择 `将所有的证书都放入下列存储(P)` 。



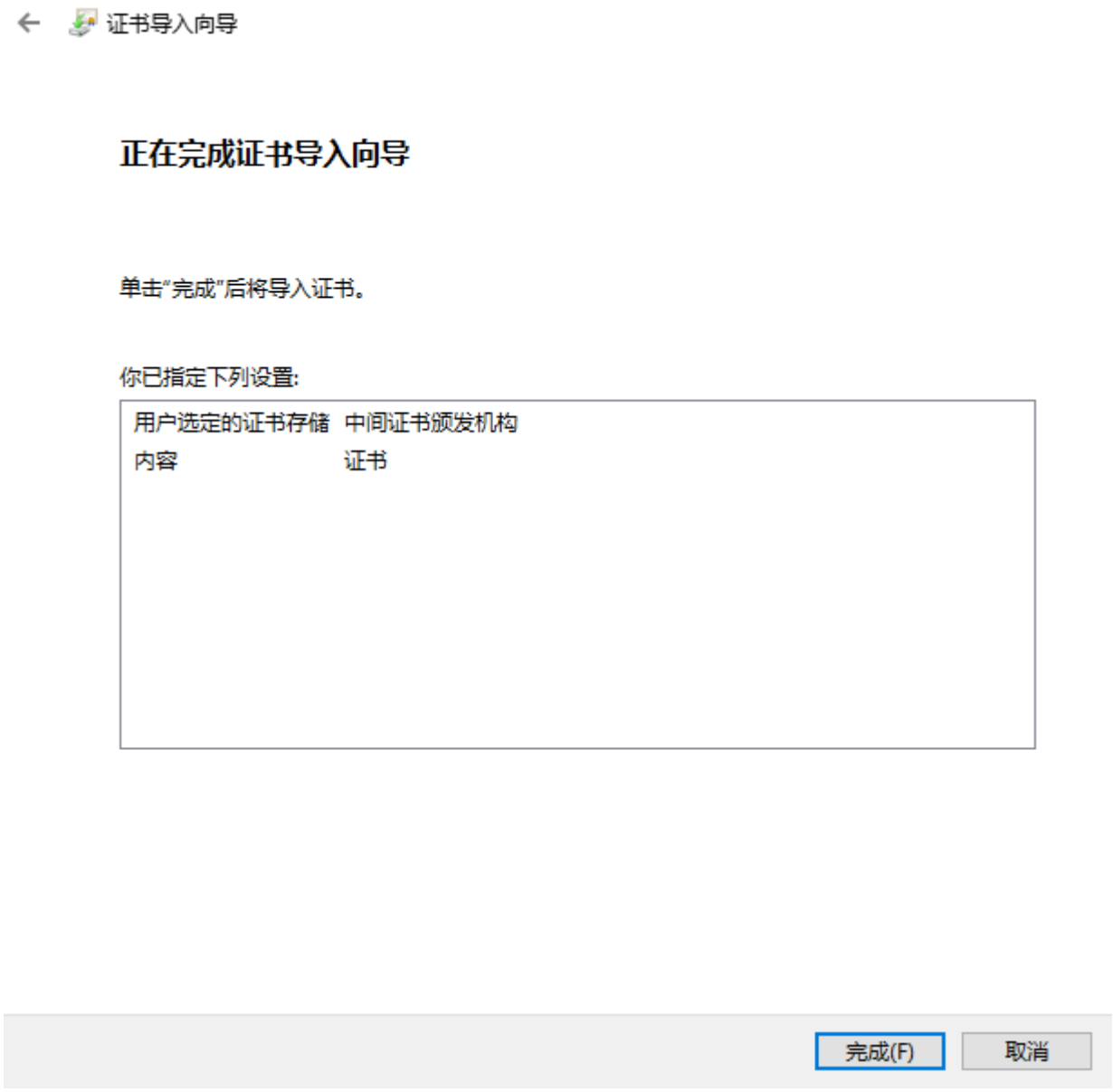
5. 单击 `浏览` ，如果是根CA选择 `受信任的根证书颁发机构` ，如果是从属CA选择 `中间证书颁发机构` 。选择完成后单击 `确定` 。


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

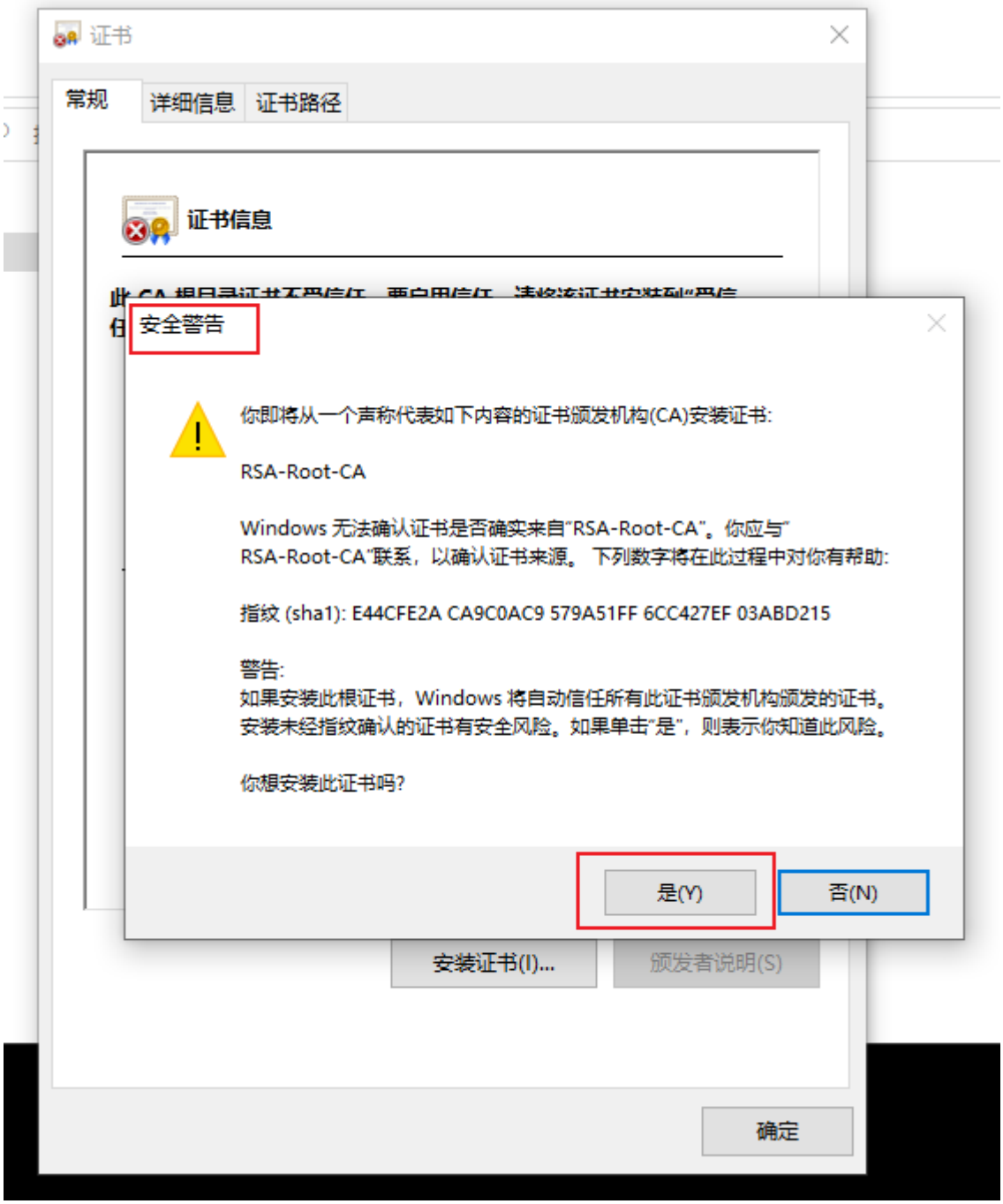
6. 单击 `下一页` 。

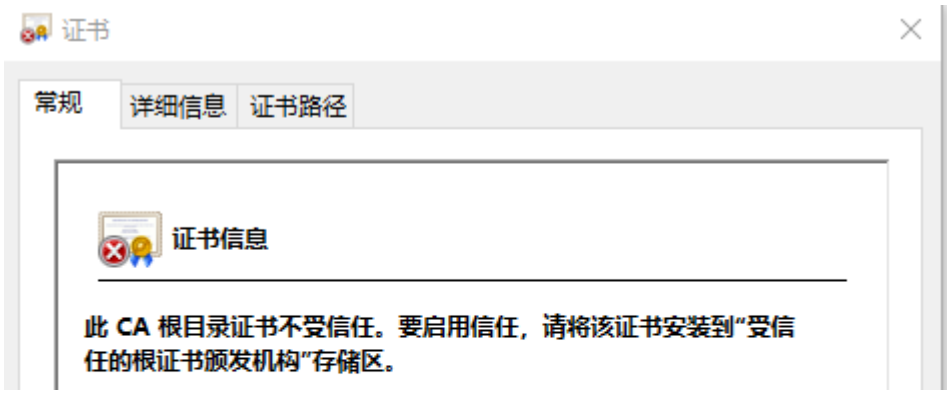


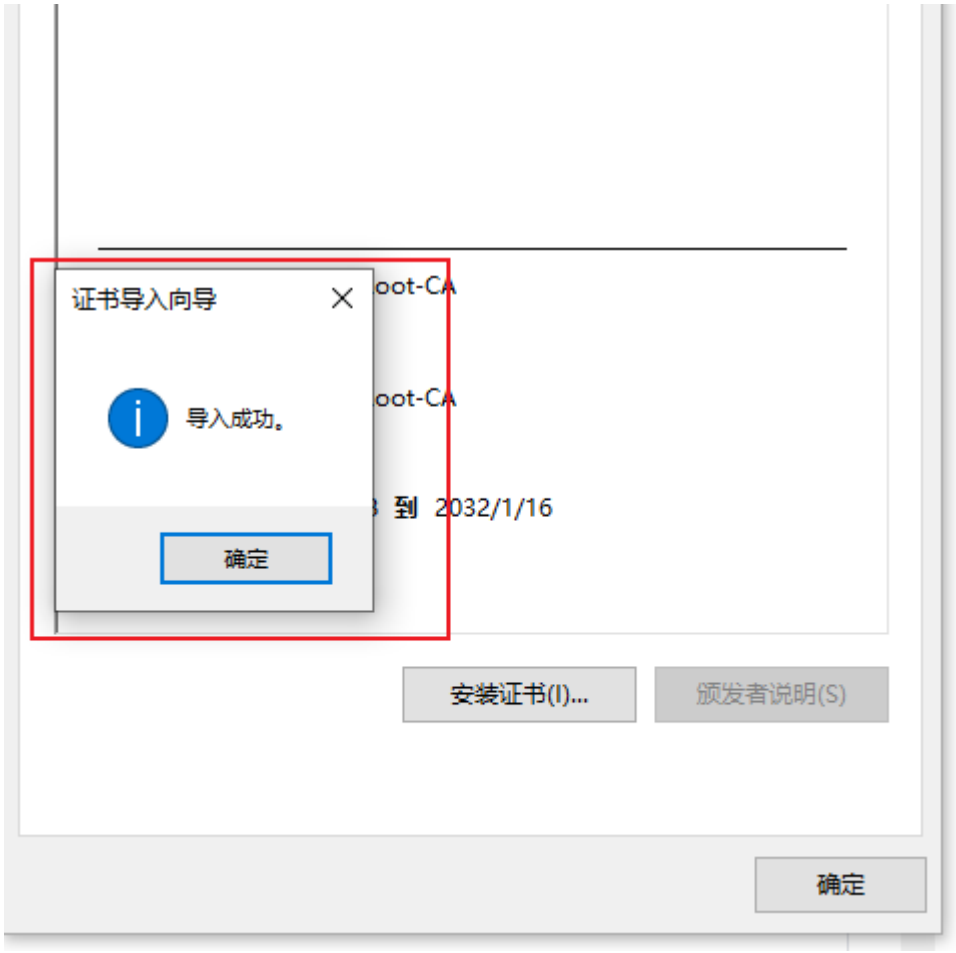
7. 单击 `完成` ，弹出安全警告窗口。


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。



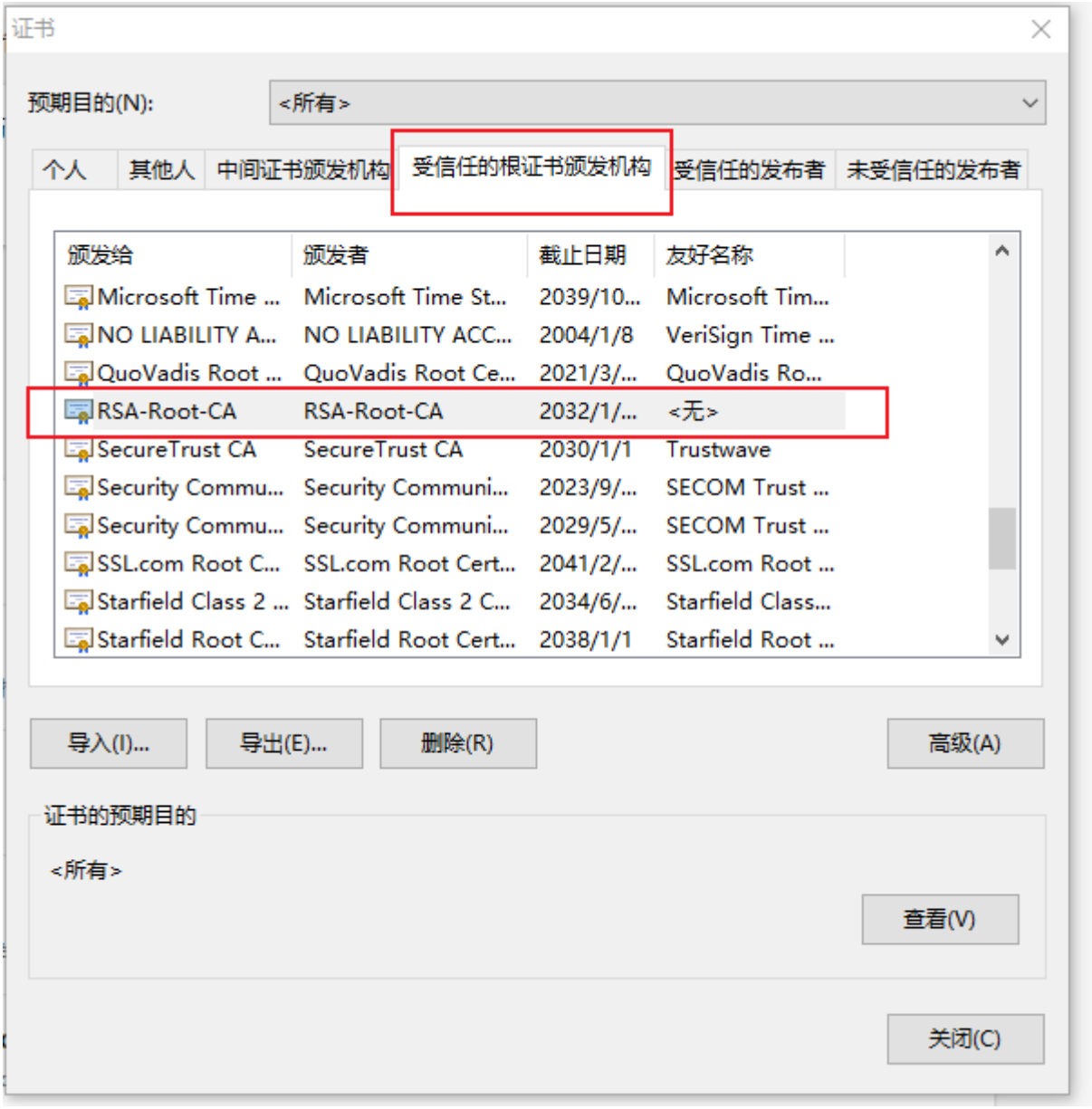
9. 重复以上步骤，依次安装该私有证书的签发CA到根CA的所有CA证书。

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。

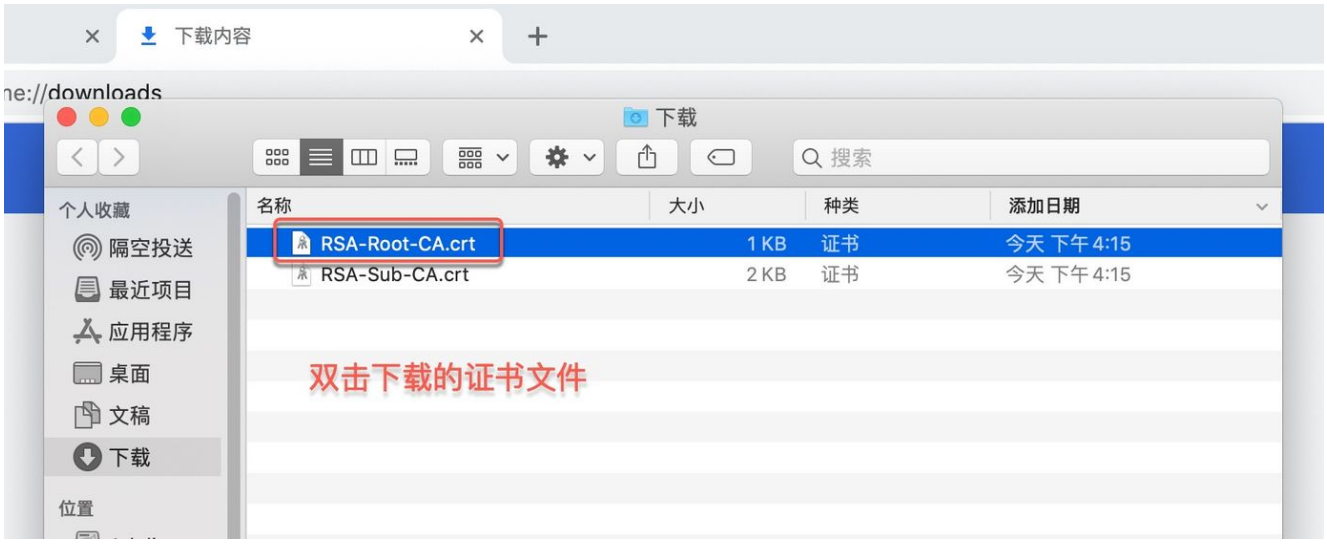


macOS操作系统

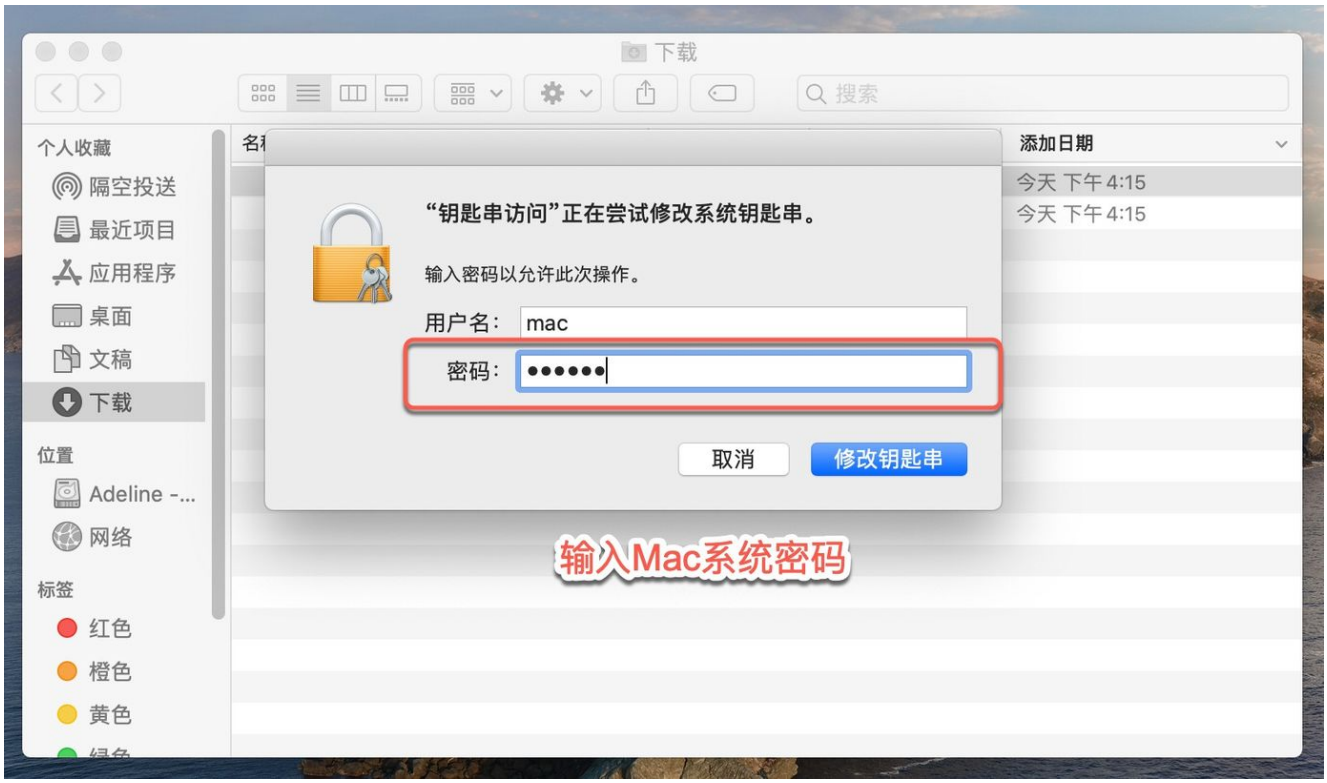
本节介绍在macOS操作系统中，如何导入私有证书的签发CA证书链，使其成为受信任的证书颁发机构。

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。

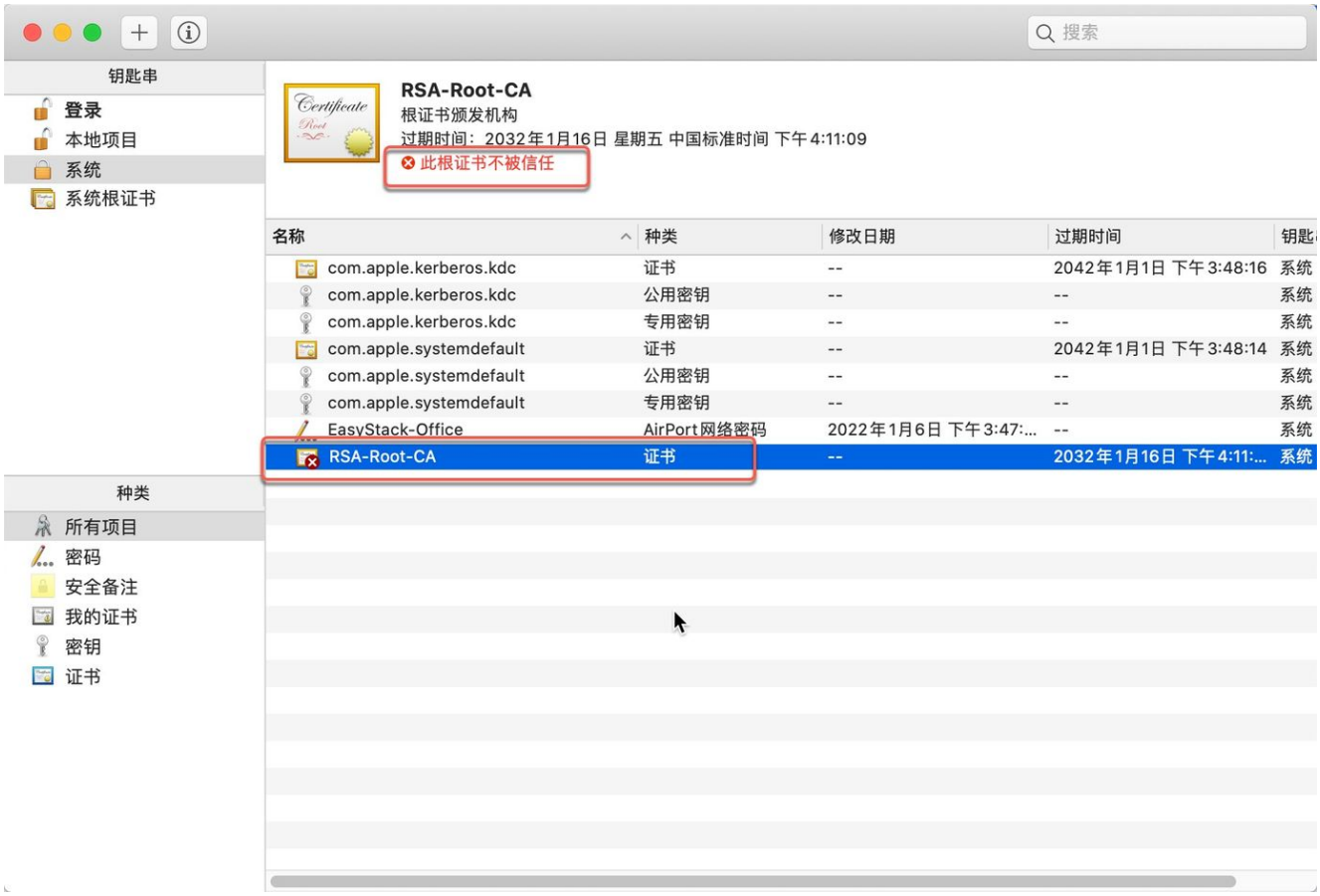
2. 双击某个证书文件，弹出密码输入窗口。



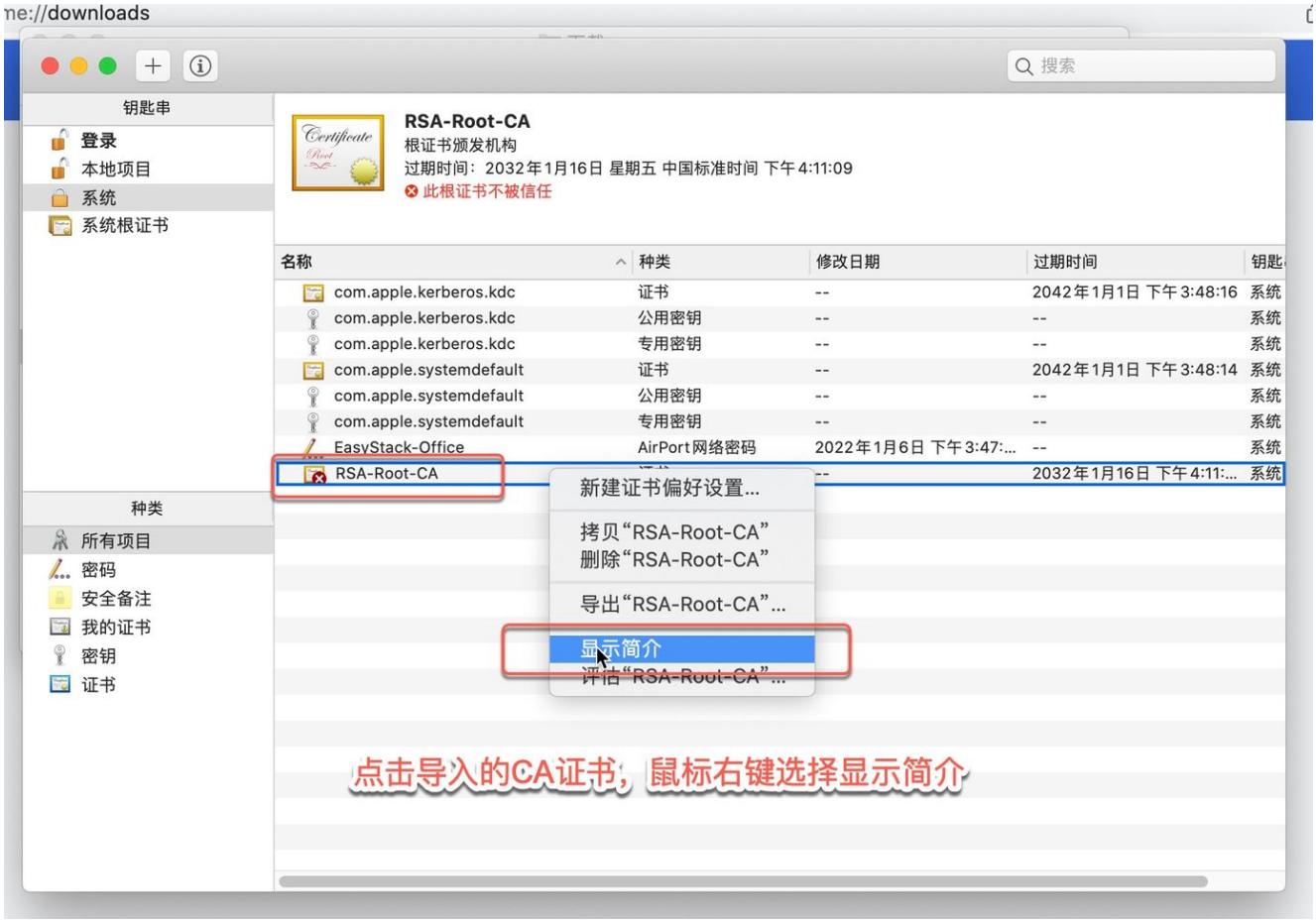
3. 输入系统密码，单击 修改钥匙串 ，弹出钥匙串列表。



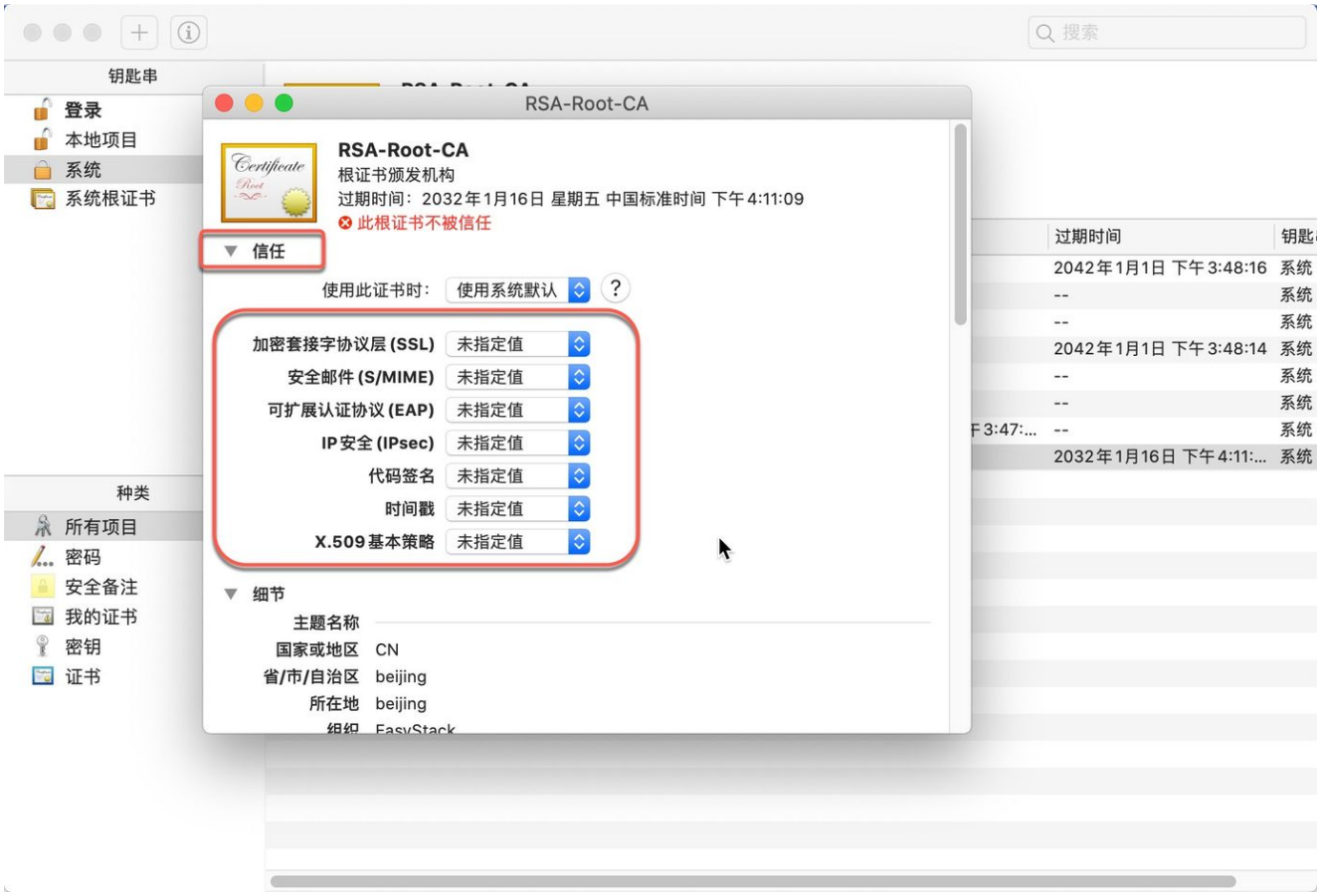
4. 此时虽然私有CA的证书已经导入到系统钥匙串中，但仍不受系统信任。



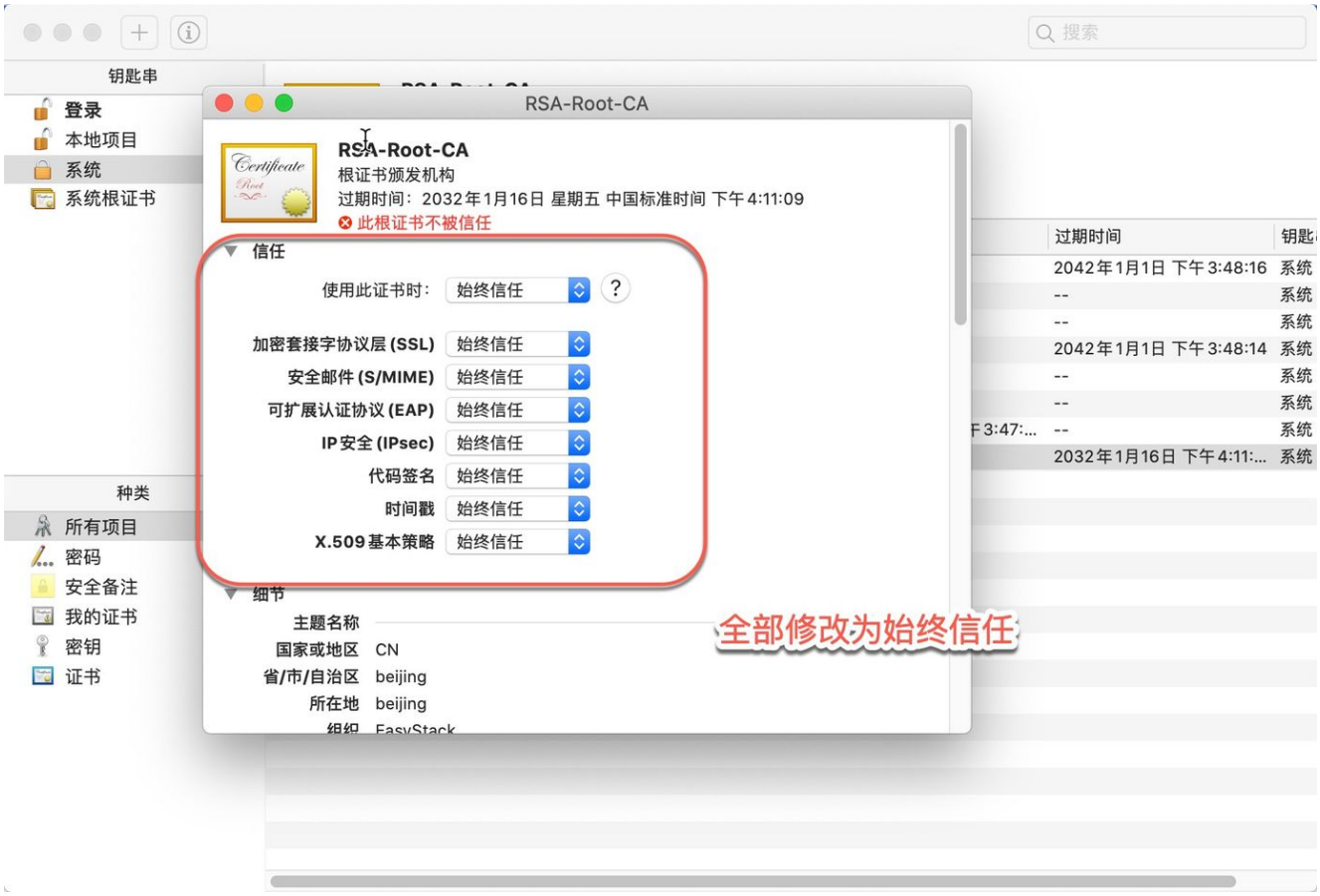
5. 右键单击导入的私有CA证书，选择“显示简介”。



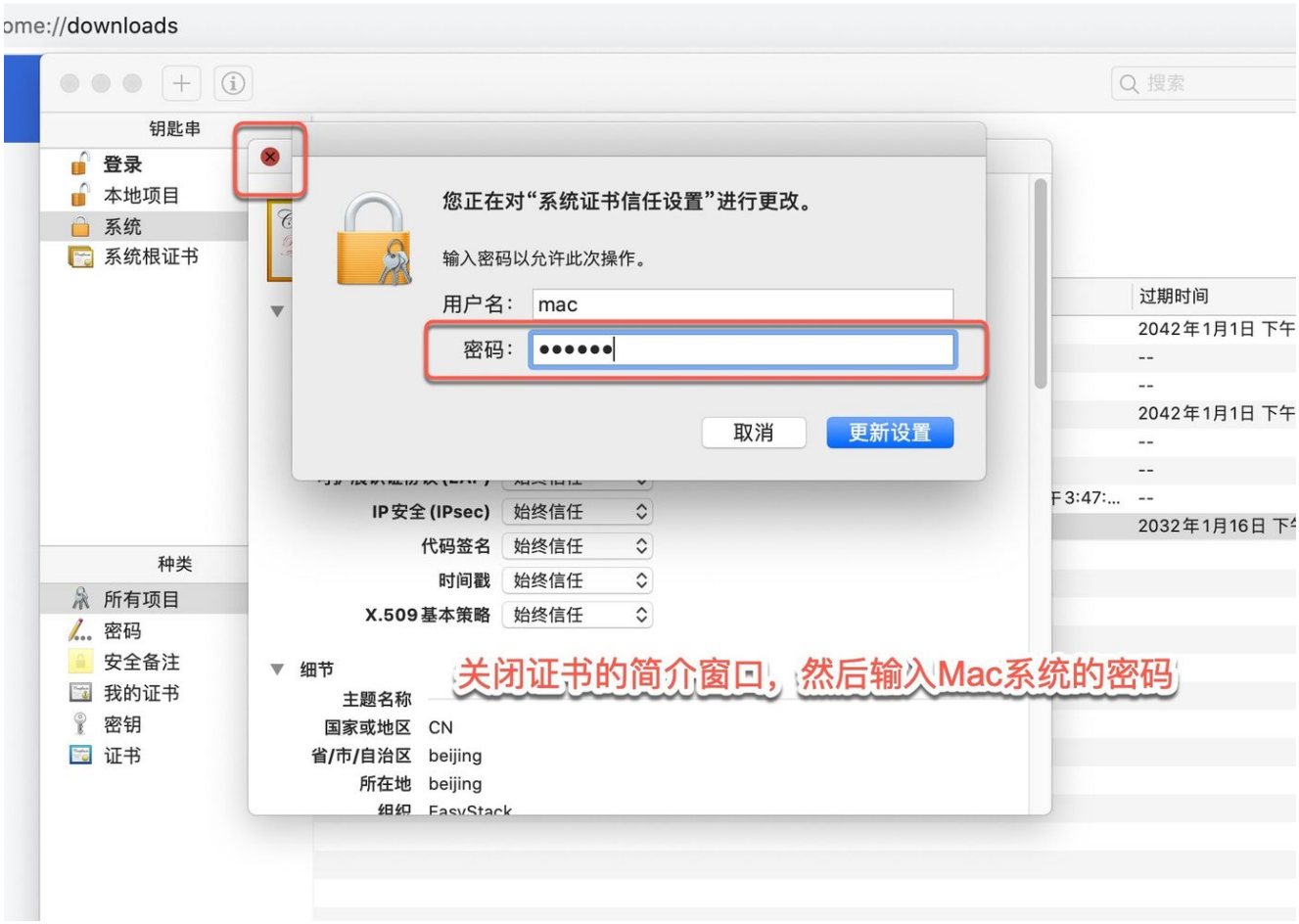
6. 展开“信任”下的详细信息。



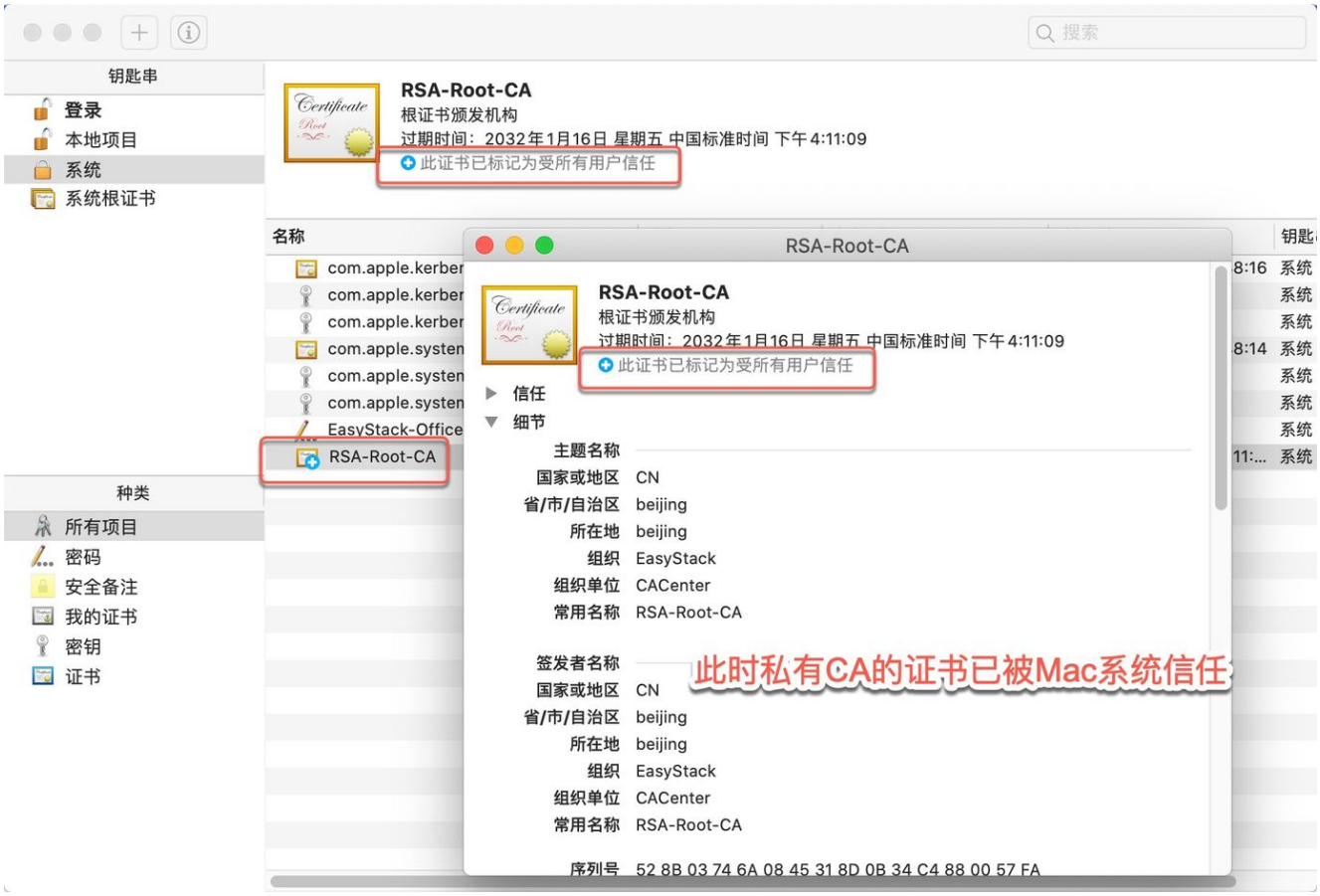
7. 将详细信息中的所有选项改为“始终信任”。



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。



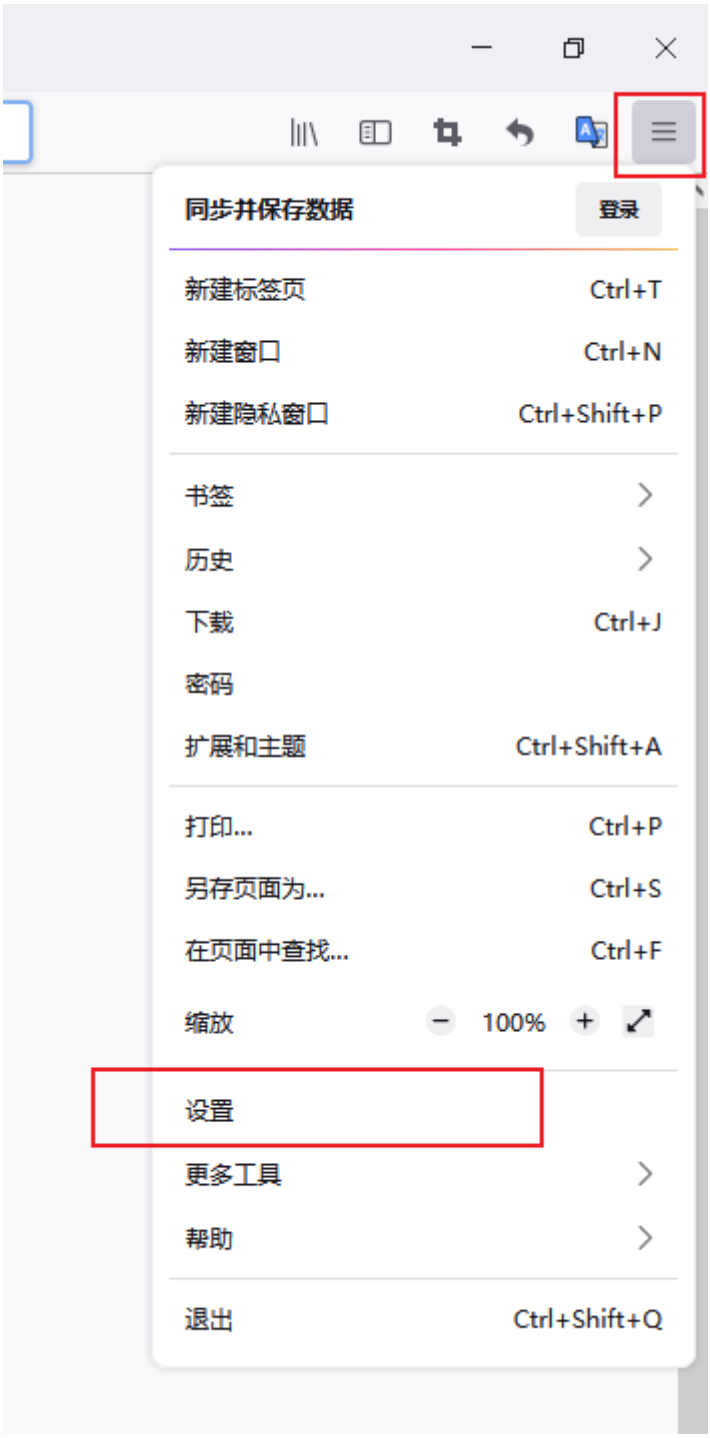
9. 再次在钥匙串列表中查看导入的私有CA证书，已被系统信任。



Firefox浏览器

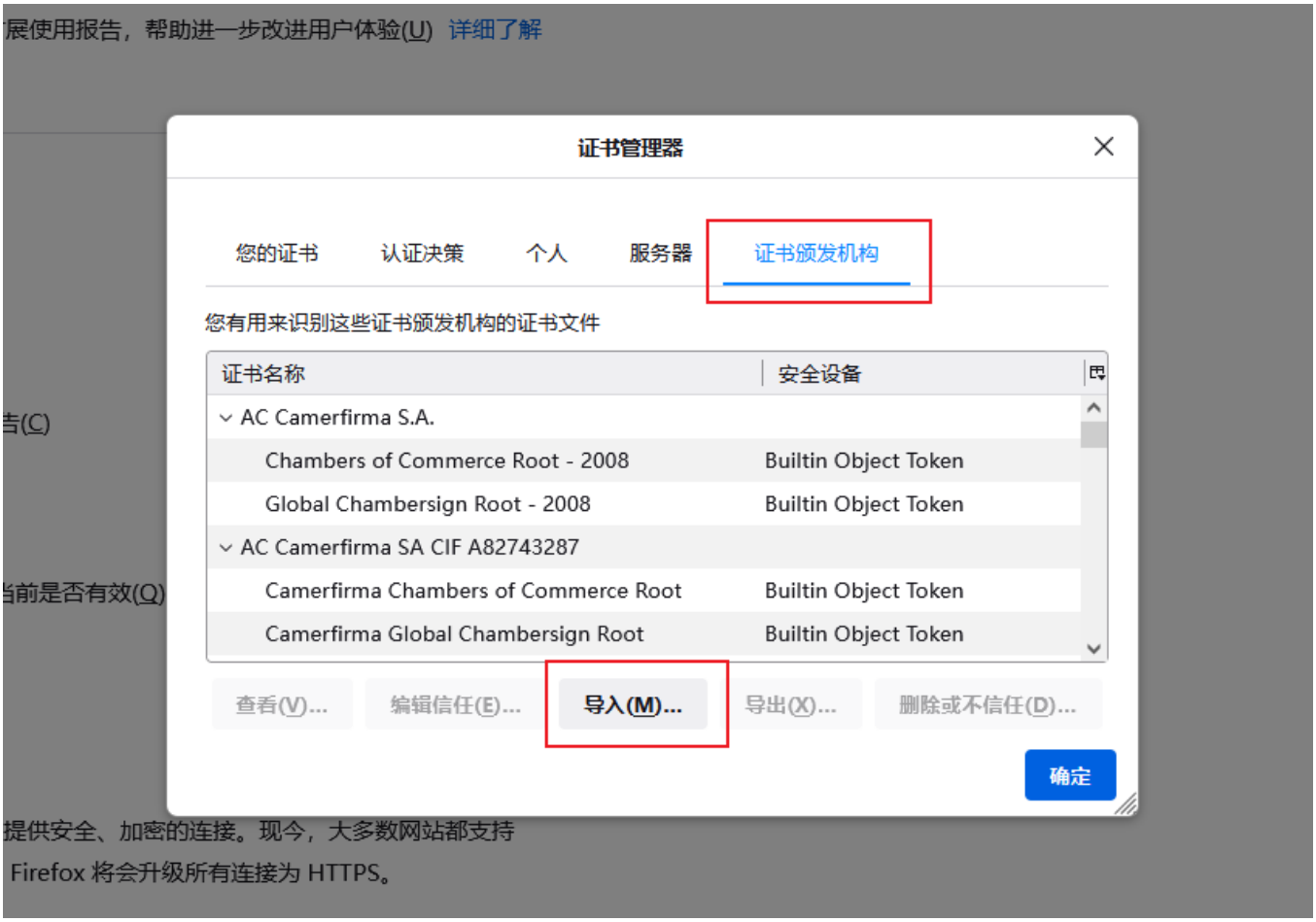
本节介绍如何在Firefox浏览器中导入私有证书的签发CA证书链，使其成为受信任的证书颁发机构。

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。

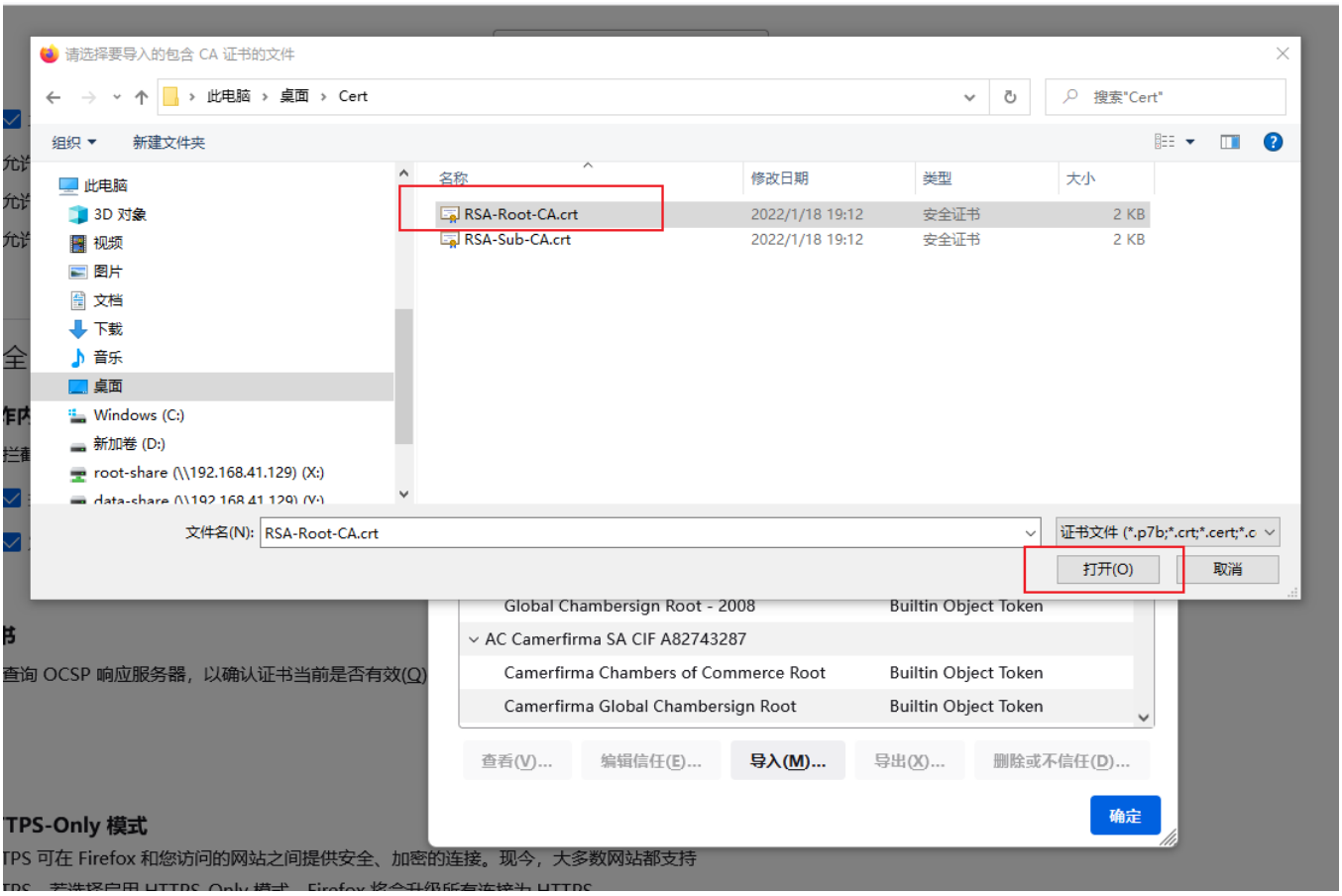


3. 在“隐私与安全”菜单项中，找到“证书”，单击 查看证书 。

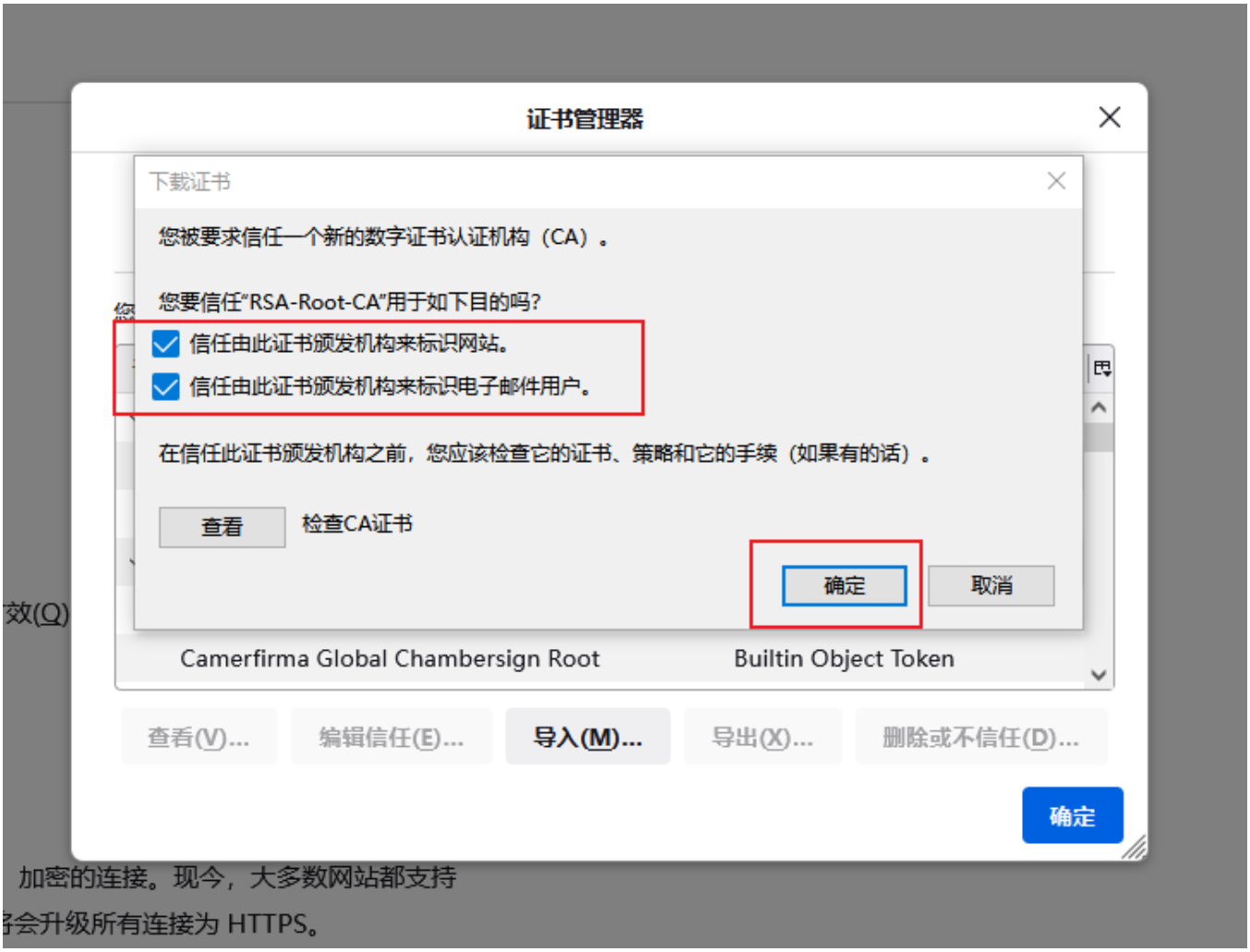
4. 在弹出的证书管理器中，选择“证书颁发机构”页签，单击 `导入` 。



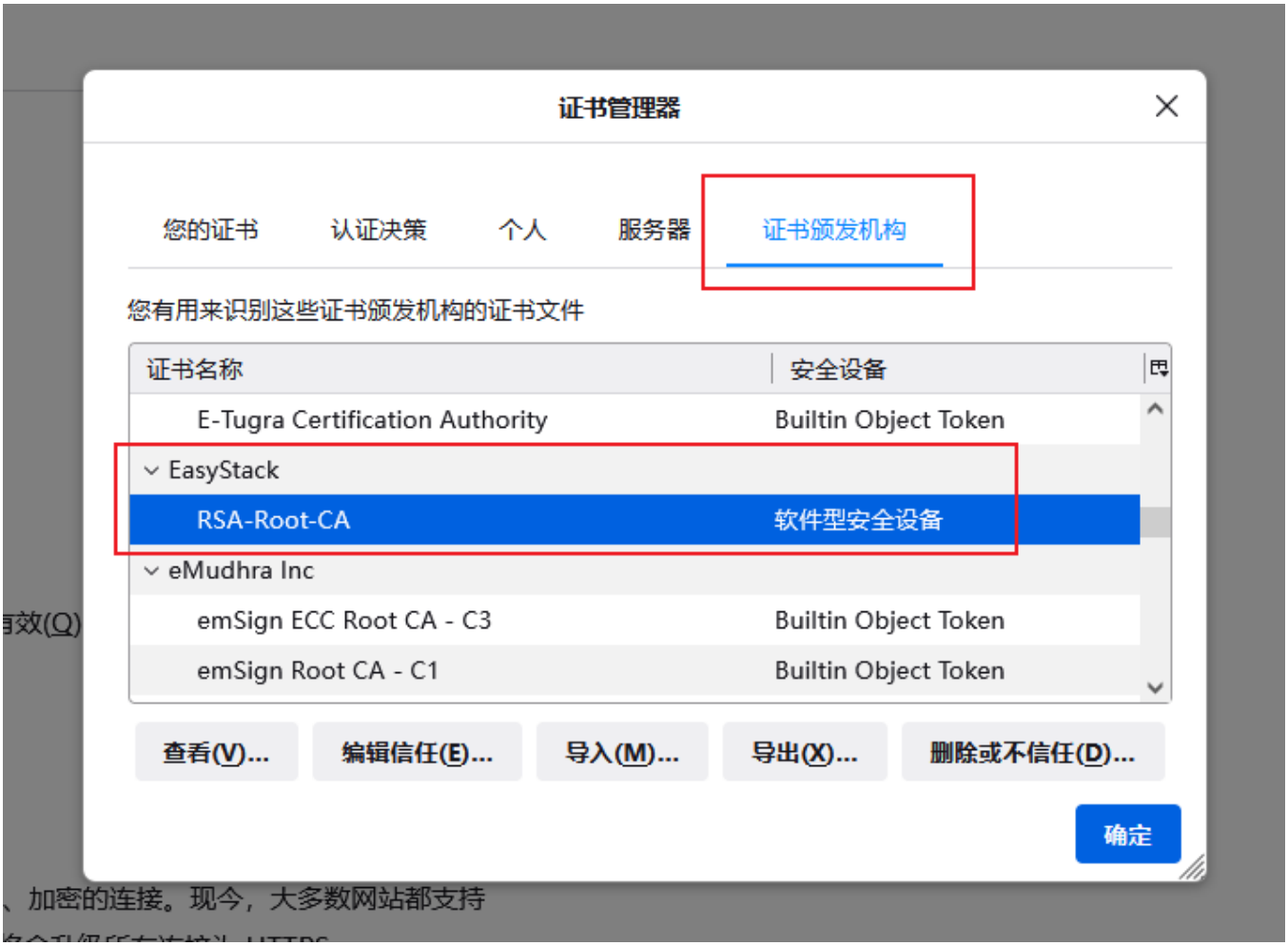
5. 选择下载好的私有CA证书文件，单击 `打开` 。



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。

5.2 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1号楼1层107-2号
南京易捷思达软件科技有限公司：
江苏省南京市雨花台区软件大道168号润和创智中心4栋109-110

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)