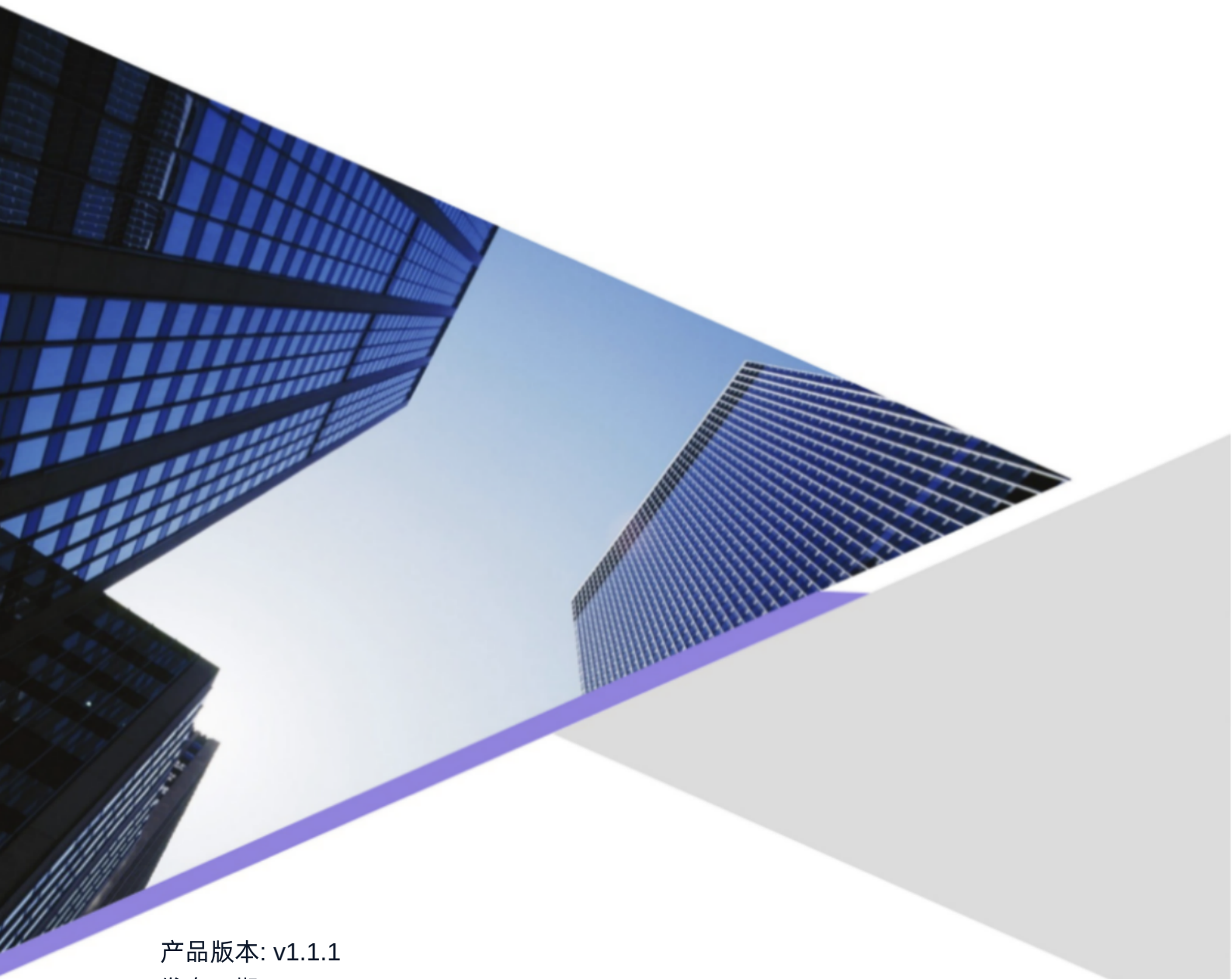
易捷行云
EasyStack

证书与密钥服务

使用手册



产品版本: v1.1.1
发布日期: 2023-06-20

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
证书与密钥服务	V1.1.1	2022-05-31

更新说明

新增功能

- 支持私有CA管理功能，搭建和维护企业的CA基础设施，包括建立完整的CA层次体系，如根CA和从属CA，提供私有CA全生命周期管理如创建、编辑、删除、禁用、启用等。
- 支持多种密钥算法，支持 RSA2048、RSA4096、ECC256、ECC384、国密SM2，满足国密要求规范。
- 支持SHA256、SHA384、SHA512、国密SM3等多种签名哈希算法。
- 支持私有CA签发私有证书功能，提供证书全生命周期管理，满足客户对安全场景的诉求。
- 支持私有CA签发客户端证书和服务端证书。
- 支持上传已有证书，方便统一管理。
- 支持密钥管理功能，提供密钥全生命周期管理，如创建、编辑、删除、禁用、启用等。
- 支持创建密钥，实现用户级隔离的数据加密保护。
- 支持计划删除功能，高危操作防护机制，防止密钥意外删除导致数据无法解密。
- 支持根据不同的硬件厂商加密机，动态返回支持的密钥算法，包括对称密钥、非对称密钥以及国密算法。
- 支持加密、解密、签名、验签 API能力，方便云产品在集成安全特性时调用并具备数据加解密能力。

依赖说明

- 安装本产品前需确保平台版本>=6.0.2。

2 产品介绍

2.1 什么是证书与密钥服务

证书与密钥服务是平台上提供私有CA、数字证书及密钥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与密钥，托管企业购买的或第三方生成的证书。证书与密钥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

- **证书与密钥全生命周期管理**

  集成证书服务与密钥服务的一体化产品，可以通过简单的可视化操作建立完整的CA体系及密钥体系，并对其进行全生命周期的管理。

- **多种密钥算法支持**

  证书服务不仅支持RSA2048、RSA4096、ECC256、ECC384等多种国际密钥算法，符合PKI/CA国际标准，还支持SM2、SM3等国密算法。

  密钥服务不仅支持AES_256、RSA_2048、RSA_3072、RSA_4096、EC_P256、EC_P384等国际算法，还支持SM2、SM4等国密算法。

- **双证书机制**

  支持签发双证书，即使用国密算法生成的签名证书和加密证书。签名证书在签名时使用，仅用来验证身份，加密证书在密钥协商时使用，其私钥和公钥由CA产生，并由CA保管。

- **证书托管**

  通过将本地的证书上传到证书服务，可以实现用户对证书的统一管理。

- **与云产品无缝集成**

  证书服务与独享型负载均衡云产品深度集成后，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。

密钥服务与身份与访问管理、计算、镜像、块存储等云产品集成后，可以统一管理用户的所有密钥，还可以进行本地数据的加解密和签名验签。

- **投入成本降低**

  私有证书服务能够避免高昂的商业证书开销，尤其在开发、测试阶段，通过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。

  密钥服务提供统一的密钥管理策略和加密API给云产品服务使用，用户无需自建密码基础设施。

- **安全合规**

  密钥服务的密钥都由符合国家密码管理局认证的硬件加密机来执行密码学运算生成和存储，保证密钥的安全性和合规要求。

  私有CA服务能够签发客户端证书和服务端证书，提供端到端的加密，满足客户对安全场景的诉求。

主要功能

私有CA

- 支持私有证书颁发机构（私有CA），支持多种密钥算法，包括RSA2048、RSA4096、ECC256、ECC384、SM2，支持X.509 v3证书格式。
- 支持根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。
- 支持CA的全生命周期管理，包括启动、禁用、删除、下载等操作。

证书管理

- 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、SM2。
- 支持证书文件格式适配多种服务器类型，例如Tomcat、Nginx、Apache、IIS。
- 支持上传第三方生成的证书和私钥功能，实现在云平台统一管理各种证书、查看绑定证书域名和到期时间、修改证书名称、删除过期的证书等一站式服务，有效提高证书运维效率。

密钥管理

- 支持密钥产生、保存、分发和销毁等全生命周期的管理。
- 创建密钥支持多种密钥算法，包括AES_256、RSA_2048、RSA_3072、RSA_4096、EC_P256、EC_P384等国际算法，以及SM2、SM4等国密算法，实现用户级隔离的数据加密保护。
- 支持信封加密，基于密钥管理系统的信封加密能力，可以对任意长度或大小的数据进行加密。
- 支持根据不同厂商的硬件加密机，动态返回密钥算法，包括对称密钥、非对称密钥以及Hash算法。
- 支持密钥计划删除功能，高危操作防护机制，防止密钥意外删除导致数据无法解密。

2.2 使用场景

- **保护企业信息化应用**

  建立统一的企业证书管理体系，实现证书全生命周期管理，融入持续监控和自动化管理能力，防范因证书管理不善导致的风险。并可以使用证书在企业内部进行应用身份认证和数据加解密。

- **数字身份认证**

  客户端证书是相对于服务器端而言，是用于证明客户端用户身份的数字证书，用户在与服务器端通信时可以证明其真实身份。适用于各种涉密系统、网上应用和网络资源的客户端强身份认证。

  客户端证书是一种更加安全的数字身份认证，通过客户端证书来代替用户名密码的形式安全地访问系统。

- **VPN Server使用客户端证书认证**

  VPN Server使用客户端证书认证机制替代传统的用户名和密码等形式，提升VPN安全，保护组织内部系统。

- **保护云平台服务数据的机密性和完整性**

  密钥服务的密钥使用经过国家密码管理局鉴定通过的硬件密码设备来生成和保护，使用密钥服务轻松创建和控制用于加密数据的密钥，与多个云产品服务集成，以帮助客户保护这些服务数据的机密性和完整性。

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，可划分密钥类型为对称加密和非对称加密两种。即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。在本云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

前提条件

在执行下述产品获取操作步骤前，请确保以下条件均已满足：

- 如需获取正式版云产品，请提前将已获取的许可文件准备就绪。

操作步骤

1. 获取并安装“证书与密钥服务”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“证书与密钥服务”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. 访问证书与密钥服务。

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

2.5 权限说明

本章节主要用于说明证书与密钥服务各功能的用户权限范围。其中，√ 代表该类用户可对云平台内所有项目的操作对象执行此功能，**XX项目** 代表该类用户仅支持对XX项目内的操作对象执行此功能，未标注代表该类用户无权限执行此功能。

功能		云管理员	部门管理员/项目管理员/普通用户
私有CA	信息展示	√	仅已加入项目
	创建私有CA	仅Default/admin项目	
	导出	√	
	启用/禁用	√	
	编辑	√	
	下载	√	
	删除	√	
证书管理	信息展示	√	仅已加入项目
	创建私有证书	仅Default/admin项目	
	导出	√	
	上传证书	仅Default/admin项目	
	下载	√	
	编辑	√	
	删除	√	
密钥管理	信息展示	仅该用户创建对象	仅该用户创建对象

	功能	云管理员	部门管理员/项目管理员/普通用户
	创建密钥		
	编辑		
	对称密钥在线加密/解密		
	导出		
	启用/禁用		
	删除		
	取消计划删除		

2.6 使用限制

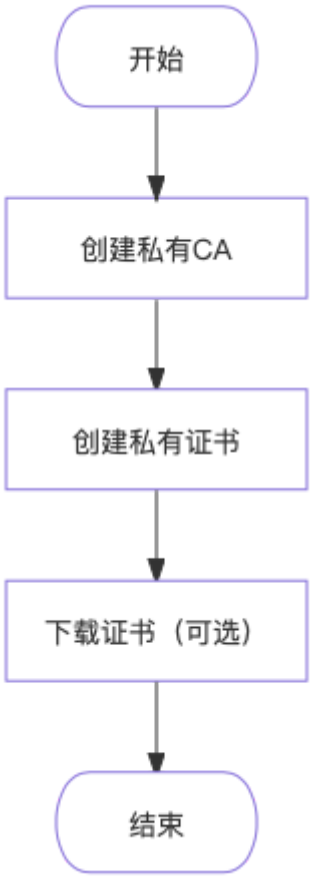
- 对于私有CA，其层级结构最多支持8级。
- 对于对称密钥在线加密/解密功能，输入的数据长度不能超过512个字符。

3 快速入门

3.1 证书服务

3.1.1 操作指引

证书服务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。

操作流程	描述
创建私有证书	确认签发CA存在后，即可创建私有证书。
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。

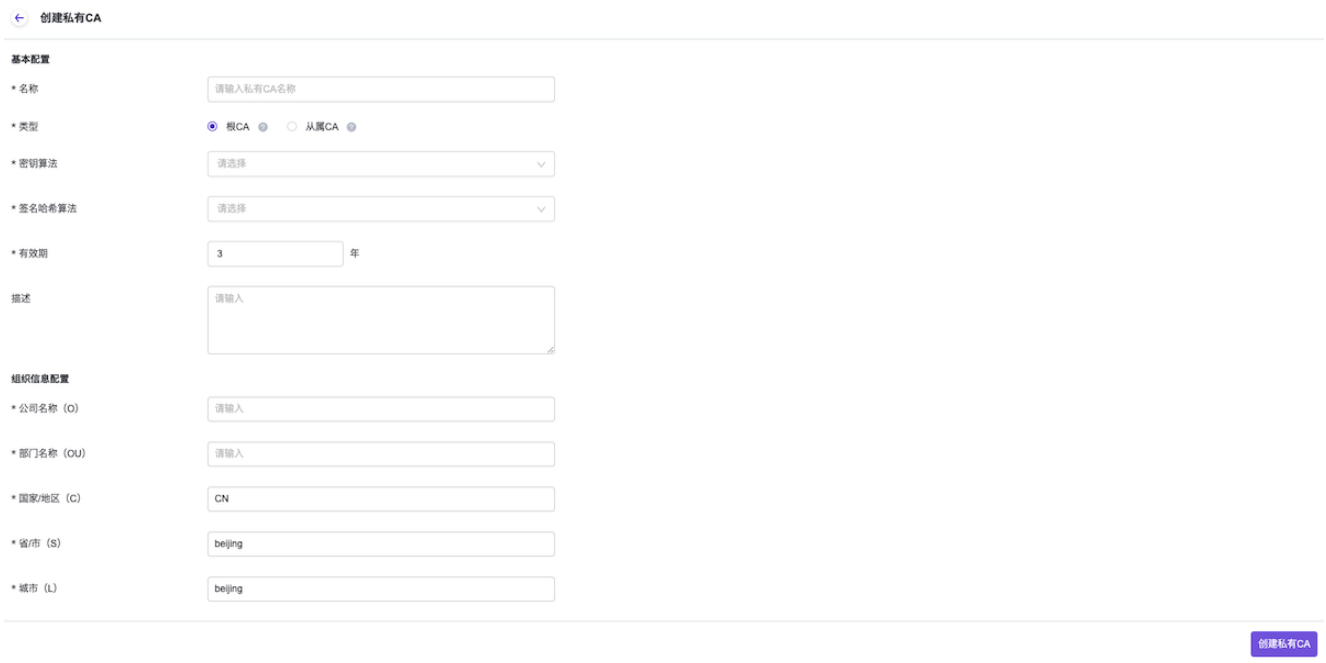
3.1.2 创建私有CA

> 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]-[证书与密钥服务]-[私有CA]，进入“私有CA”页面。

2. 单击 `创建私有CA` ，进入“创建私有CA”页面。

3. 配置参数后，单击 `创建私有CA` ，完成操作。



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。

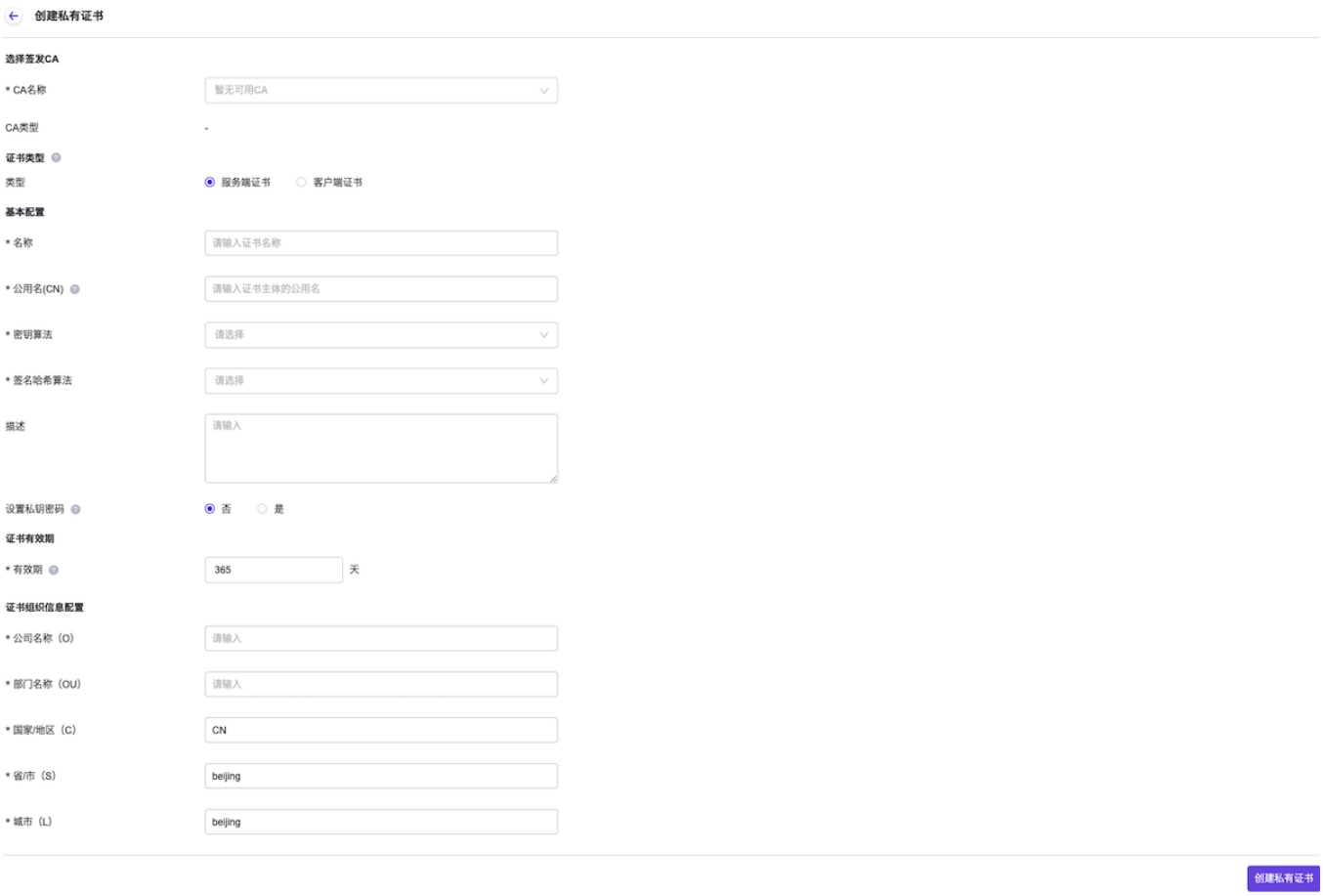
参数	说明
密钥算法	选择私有CA签发证书时所使用的加密算法类型。当前支持RSA2048、RSA4096、ECC256、ECC384、国密SM2。对于从属CA，若其签发CA使用的是国密SM2算法，则从属CA只能使用相同算法。
签名哈希算法	选择私有CA签发证书时所使用的哈希算法类型。当前支持SHA256、SHA384、SHA512、国密SM3。当且仅当“密钥算法”参数选择了“国密SM2”时，本参数可选择“国密SM3”。
有效期	根CA有效期的取值范围为3至30年。从属CA有效期的取值范围为1至20年，同时，不能超过其签发CA的剩余有效期。有效期不足1年时，无法签发从属CA。有效期结束后私有CA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	

3.1.3 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]-[证书与密钥服务]-[证书管理]，进入“证书管理”页面。
2. 单击 `创建私有证书` ，进入“创建私有证书”页面。
3. 配置参数后，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	

3.1.4 下载证书（可选）

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]-[证书与密钥服务]-[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。

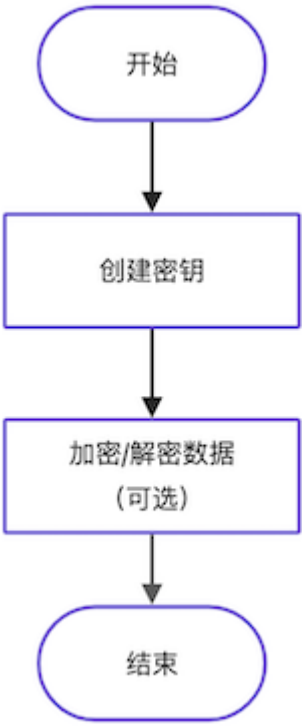
使用国密密钥算法的证书文件说明：

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

3.2 密钥服务

3.2.1 操作指引

密钥服务的主线使用流程及具体说明如下：



操作流程	描述
创建密钥	依据客户实际业务需求，创建对应类型的密钥。即当加解密需要使用相同的密钥时，请创建对称密钥，否则请创建非对称密钥。
加密/解密数据（可选）	当所创建密钥的类型为对称密钥时，可以在云平台中通过在线工具，对数据执行加密或解密操作。

3.2.2 创建密钥

本操作用于在云平台中依据客户实际业务需求，创建对应类型的密钥。即当加解密需要使用相同的密钥时，请创建对称密钥，否则请创建非对称密钥。

1. 在顶部导航栏中，依次选择[产品与服务]-[证书与密钥服务]-[密钥管理]，进入“密钥管理”页面。

2. 单击 `创建密钥` ，弹出“创建密钥”对话框。

3. 配置参数后，单击 `确认` ，完成操作。

参数	说明
名称	该密钥的名称。
保护级别	该密钥的保护级别。该参数值可选Software或HSM。 * Software：通过软件密码模块对密钥进行保护。 * HSM：Hardware Security Module（硬件安全模块），通过专用硬件对密钥进行高安全等级保护，即密钥的产生和运算都在加密机中进行。
密钥算法	该密钥的算法。 * 当“保护级别”选择“Software”时，该参数值可以选择“AES_256”（对称密钥），用于加密解密，也可以选择“ RSA_2048”（非对称密钥），用于签名验签。 * 当“保护级别”选择“HSM”时，密钥算法和用途将依赖加密机动态获取。
密钥类型（不可编辑）	该密钥的类型。 该参数值会根据所选的密钥算法，自动配置为“对称密钥”或“非对称密钥”，而无需手动配置，且也不支持编辑。
密钥用途	该密钥的用途。 该参数值可选“encrypt_decrypt”，即加密解密，或“sign_verify”，即签名验签。
描述（可选）	该密钥的描述信息。

3.2.3 加密/解密数据（可选）

当所创建密钥的类型为对称密钥时，可以通过本操作在云平台中使用在线工具，对数据执行加密或解密操作。

1. 在顶部导航栏中，依次选择[产品与服务]-[证书与密钥服务]-[密钥管理]，进入“密钥管理”页面。

2. 单击密钥名称链接，进入该密钥详情页面。

3. 在“在线工具”区域框中，选择 [加密] 或 [解密] 页签。

4. 在左侧输入框中对应输入明文或密文后，单击 `执行` ，可在右侧显示框中查看到加/解密后的数据。

   单击 `复制到剪切板` ，可直接复制显示框中的加/解密后数据到剪切板中。

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]-[证书与密钥服务]-[私有CA]，即可进入“私有CA”页面。

查看详情

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。

创建私有CA

1. 在“私有CA”页面中，单击 `创建私有CA` ，进入“创建私有CA”页面。

2. 配置参数后，单击 `创建私有CA` ，完成操作。其中，各参数的具体说明，请参考 创建私有CA。

导出

在“私有CA”页面中，单击列表上方的“导出”图标，可将当前云平台所有私有CA的信息导出到CSV文件中。

启用/禁用

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` ，弹出操作提示框。
2. 单击 `启用` 或 `禁用` 完成操作。

下载

在“私有CA”页面中，单击目标私有CA操作栏的 `更多` - `下载` ，完成操作。

编辑

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` ，弹出编辑对话框。
2. 修改信息，单击 `编辑` 完成操作。

删除

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` ，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]-[证书与密钥服务]-[证书管理]，即可进入“证书管理”页面。

查看详情

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。

创建私有证书

1. 在“证书管理”页面中，单击 `创建私有证书` ，进入“创建私有证书”页面。

2. 配置参数后，单击 `创建私有证书` ，完成操作。其中，各参数的具体说明，请参考 创建私有证书。

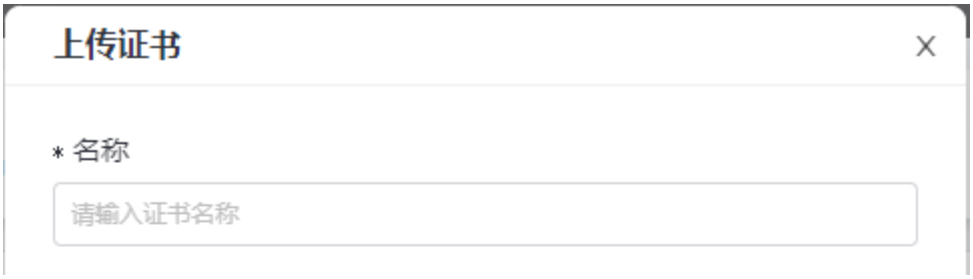
导出

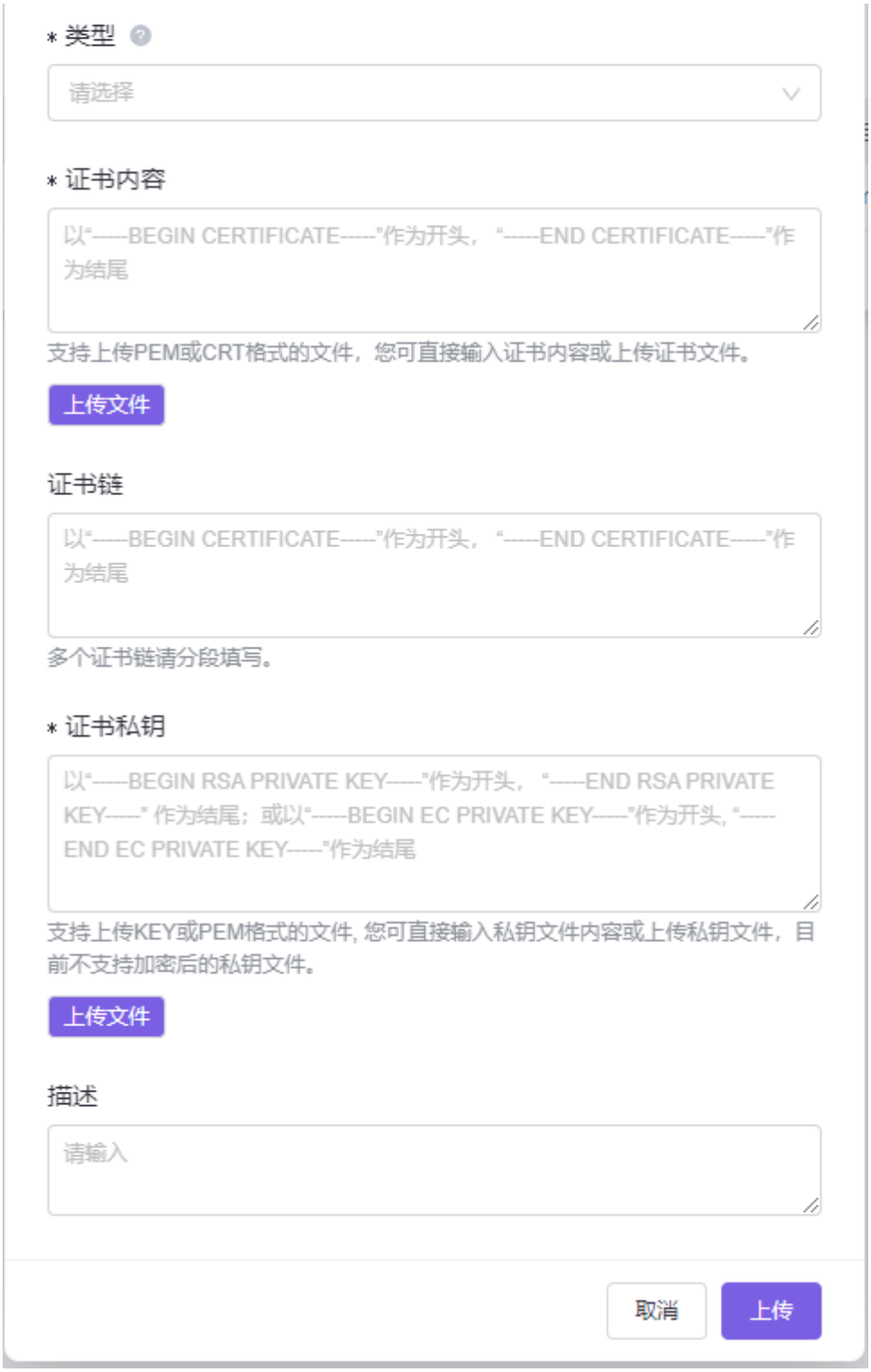
在“证书管理”页面中，单击列表上方的“导出”图标，可将当前云平台所有证书的信息导出到CSV文件中。

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。

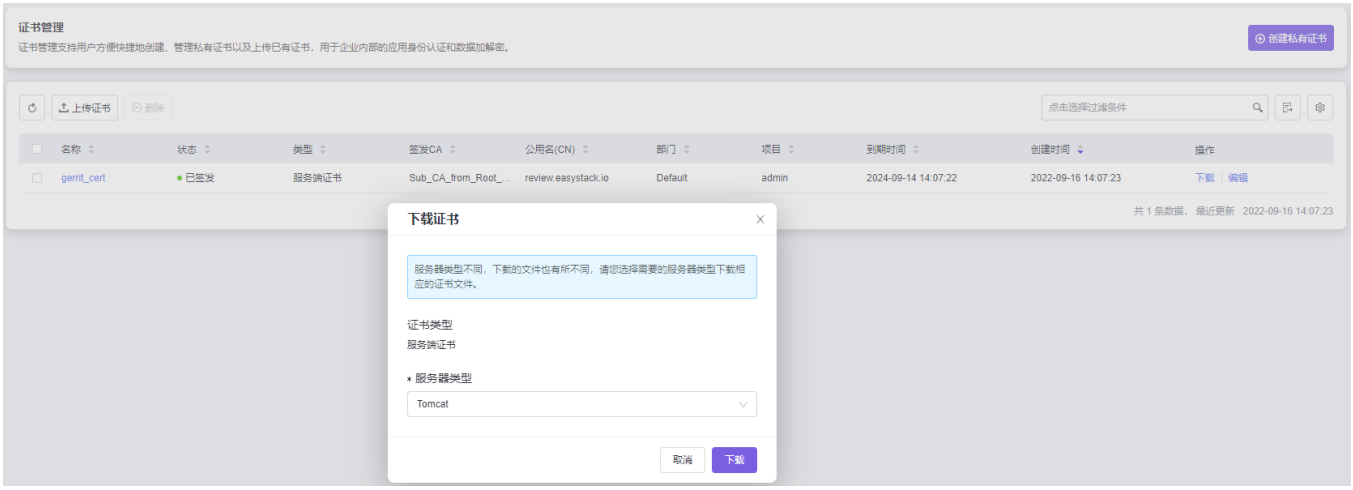




下载

1. 在“证书管理”页面中，单击目标证书操作栏的 下载 ，弹出“下载证书”对话框。

2. 选择服务器类型后，单击 下载 完成操作。



编辑

仅支持修改描述信息。

1. 在“证书管理”页面中，单击目标证书操作栏的 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

1. 在“证书管理”页面中，单击目标证书操作栏的 删除 ，或选择一个或多个待删除的证书后单击列表上方的 删除 ，弹出“删除证书”提示框。
2. 单击 删除 完成操作。

4.3 密钥管理

本章节主要介绍在“密钥管理”页面中，针对密钥的一系列运维管理操作，如：查看详情、创建密钥、启用、禁用和删除等。其中，在云平台的顶部导航栏中，依次选择[产品与服务]-[证书与密钥服务]-[密钥管理]，即可进入“密钥管理”页面。

查看详情

用于查看密钥的名称、状态、算法、类型、用途、创建时间和保护时间等详细信息。

1. 在“密钥管理”页面中，单击密钥名称链接，即可进入密钥详情页面查看信息。

在指定密钥的详情页面中，还支持对其执行编辑、在线工具加密/解密等操作。具体操作说明如下：

编辑

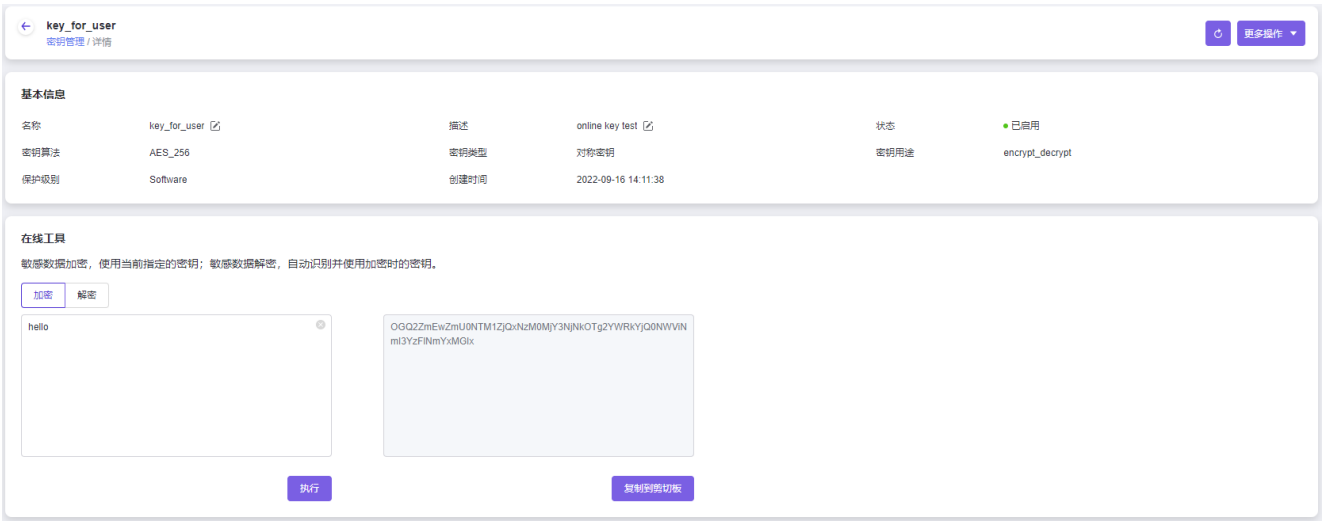
1. 在“基本信息”区域框中单击名称或描述后的“编辑”图标，或在详情页面中单击 `更多操作` - `编辑` ，弹出对应对话框。
2. 配置参数后，单击 `保存` ，完成操作。

在线工具加密/解密

对于“已启用”状态的对称密钥，支持直接使用该密钥在线对敏感数据执行加密或解密的操作。

1. 在“在线工具”区域框中，选择 [加密] 或 [解密] 页签。
2. 在左侧输入框中对应输入明文或密文后，单击 `执行` ，可在右侧显示框中查看到加/解密后的数据。

   单击 `复制到剪切板` ，可直接复制显示框中的加/解密后数据到剪切板中。



创建密钥

1. 在“密钥管理”页面中，单击 创建密钥 ，弹出“创建密钥”对话框。

2. 配置参数后，单击 确认 ，完成操作。其中，各参数的具体说明，请参考 创建密钥。

导出

在“密钥管理”页面中，单击列表上方的“导出”图标，可将当前云平台所有密钥的信息导出到CSV文件中。

启用

1. 在“密钥管理”页面中，单击目标密钥操作栏的 启用 ，弹出“启用密钥”提示框。
2. 单击 启用 ，完成操作。

禁用

本操作用于在云平台中禁用密钥。当密钥被禁用后将无法继续使用，请谨慎操作。

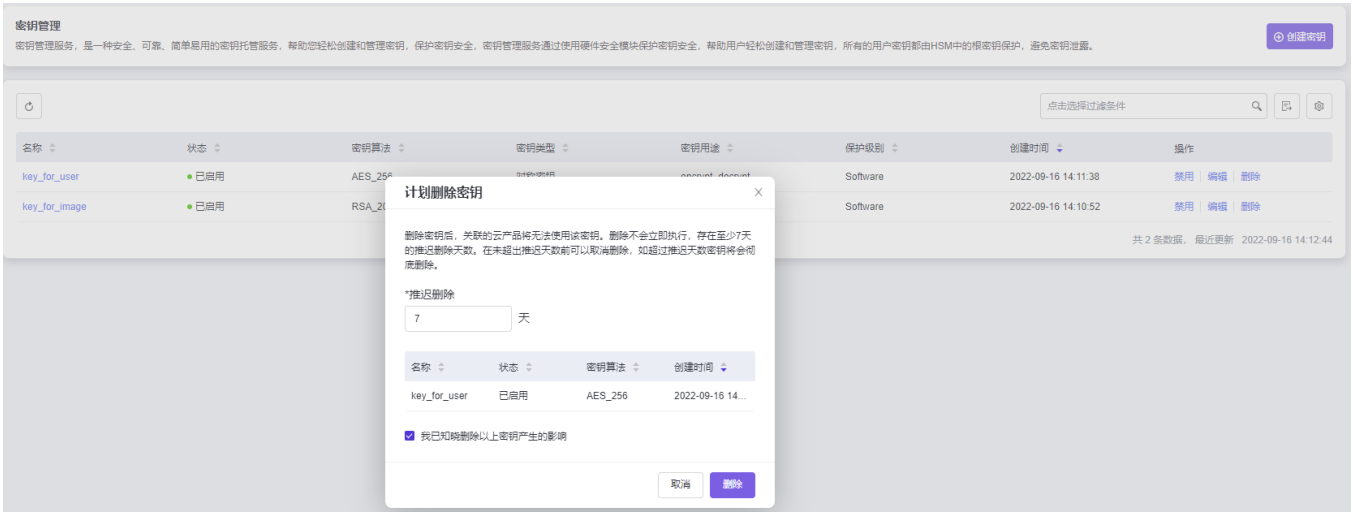
1. 在“密钥管理”页面中，单击目标密钥操作栏的 禁用 ，弹出“禁用密钥”对话框。
2. 勾选“我已知晓禁用以上密钥产生的影响”后，单击 禁用 ，完成操作。

删除

本操作用于在云平台中设置密钥删除计划。当密钥被删除后，关联的云产品将无法使用该密钥，请谨慎操作。

1. 在“密钥管理”页面中，单击目标密钥操作栏的 `删除` ，弹出“计划删除密钥”对话框。
2. 配置参数后，单击 `删除` ，完成操作。

参数	说明
推迟删除	该密钥不会在操作后便立即删除，而是在达到所设置的推迟删除天数后才会被彻底删除。 在达到推迟删除天数之前，可参考 取消计划删除 取消删除该密钥。



取消计划删除

1. 在“密钥管理”页面中，单击目标密钥操作栏的 `取消计划删除` ，弹出"取消计划删除"提示框。
2. 单击 `确认` ，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。

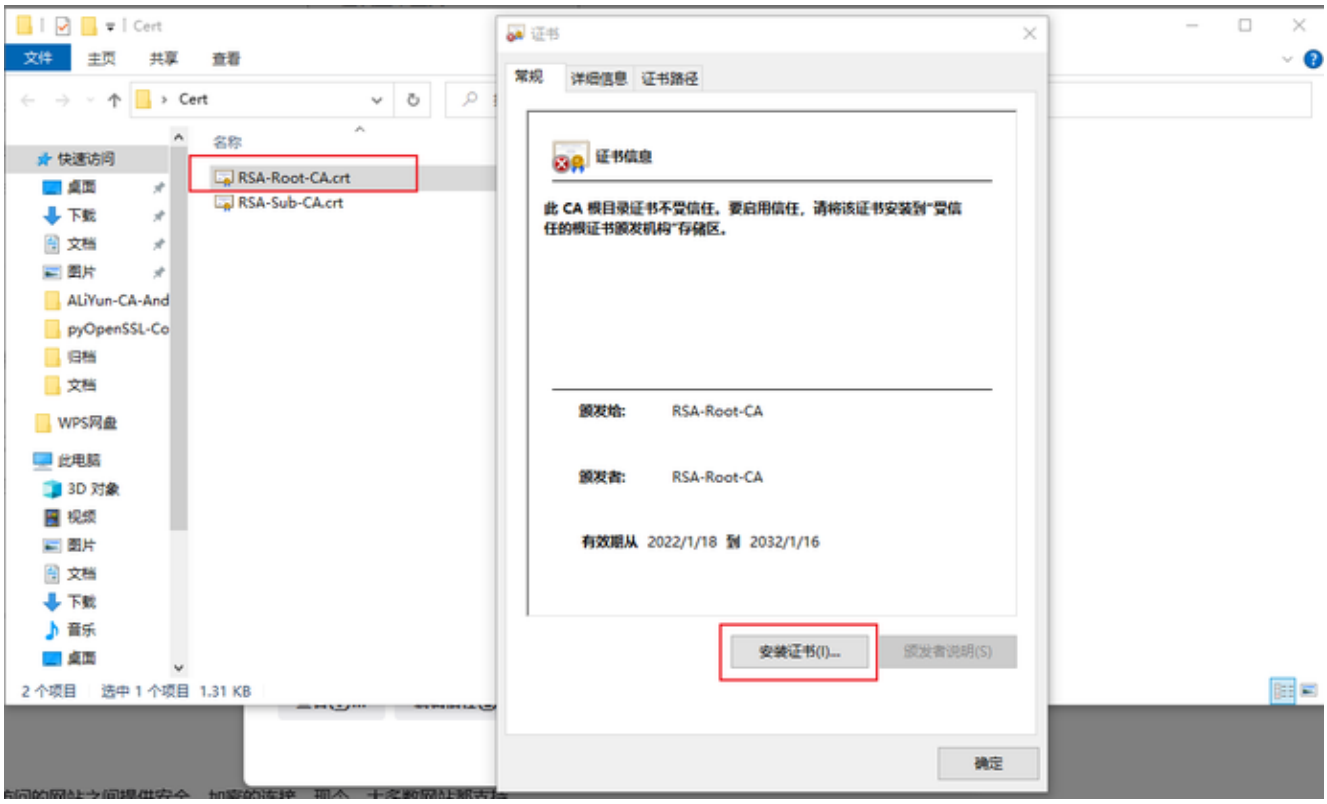
> 说明：
> Firefox浏览器是从浏览器内部的证书库检查当前证书的签发CA是否受浏览器信任，而不是读取操作系统中的证书库，因此其配置方式不同于其它浏览器。

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。

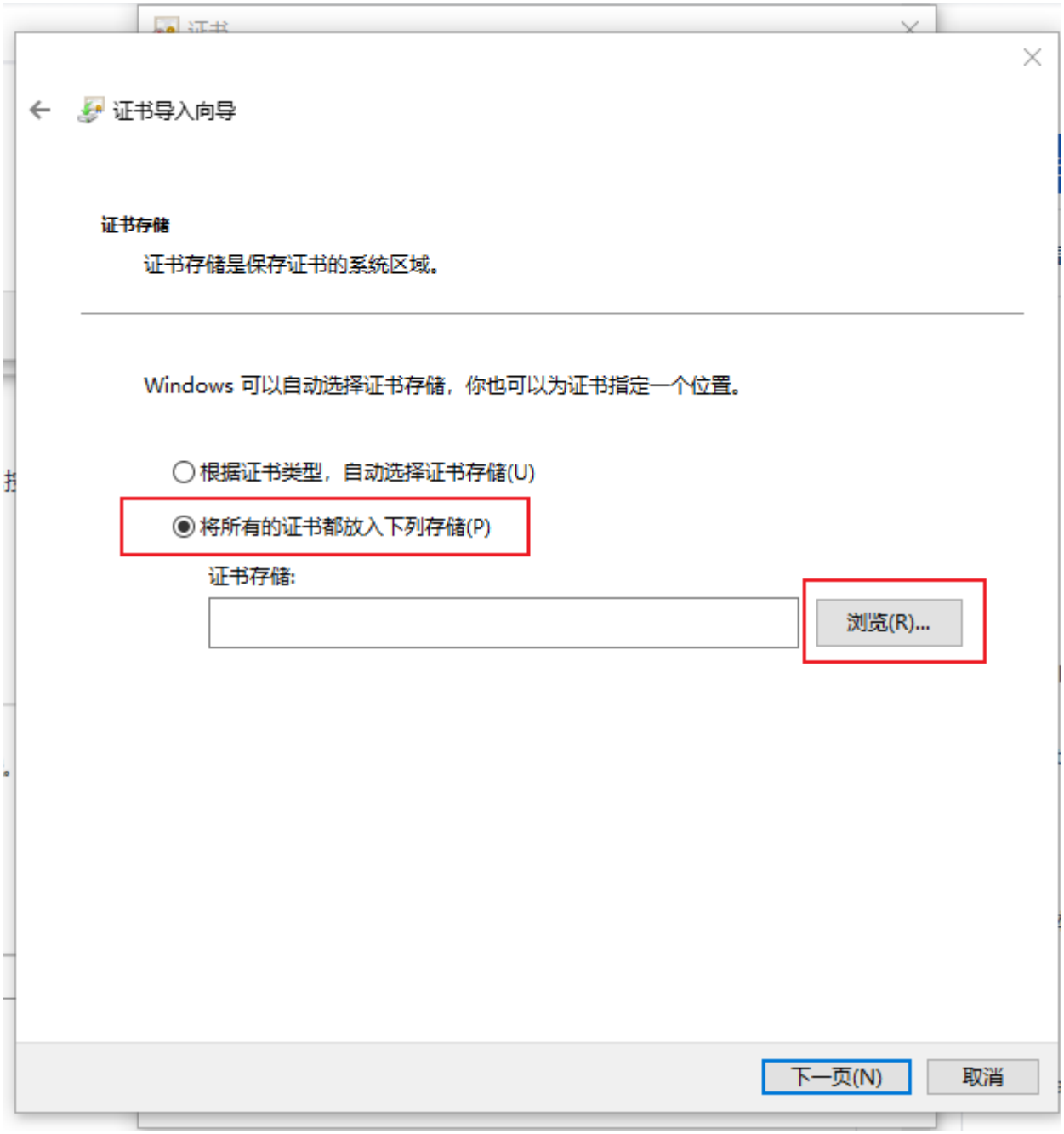
1. 在证书与密钥服务页面，下载该私有证书的签发CA链上所有的CA证书文件，即该证书的签发CA、签发CA的上一级签发CA，以此类推直至根CA。

2. 双击某个CA证书文件，在弹出的窗口中单击 `安装证书` 。

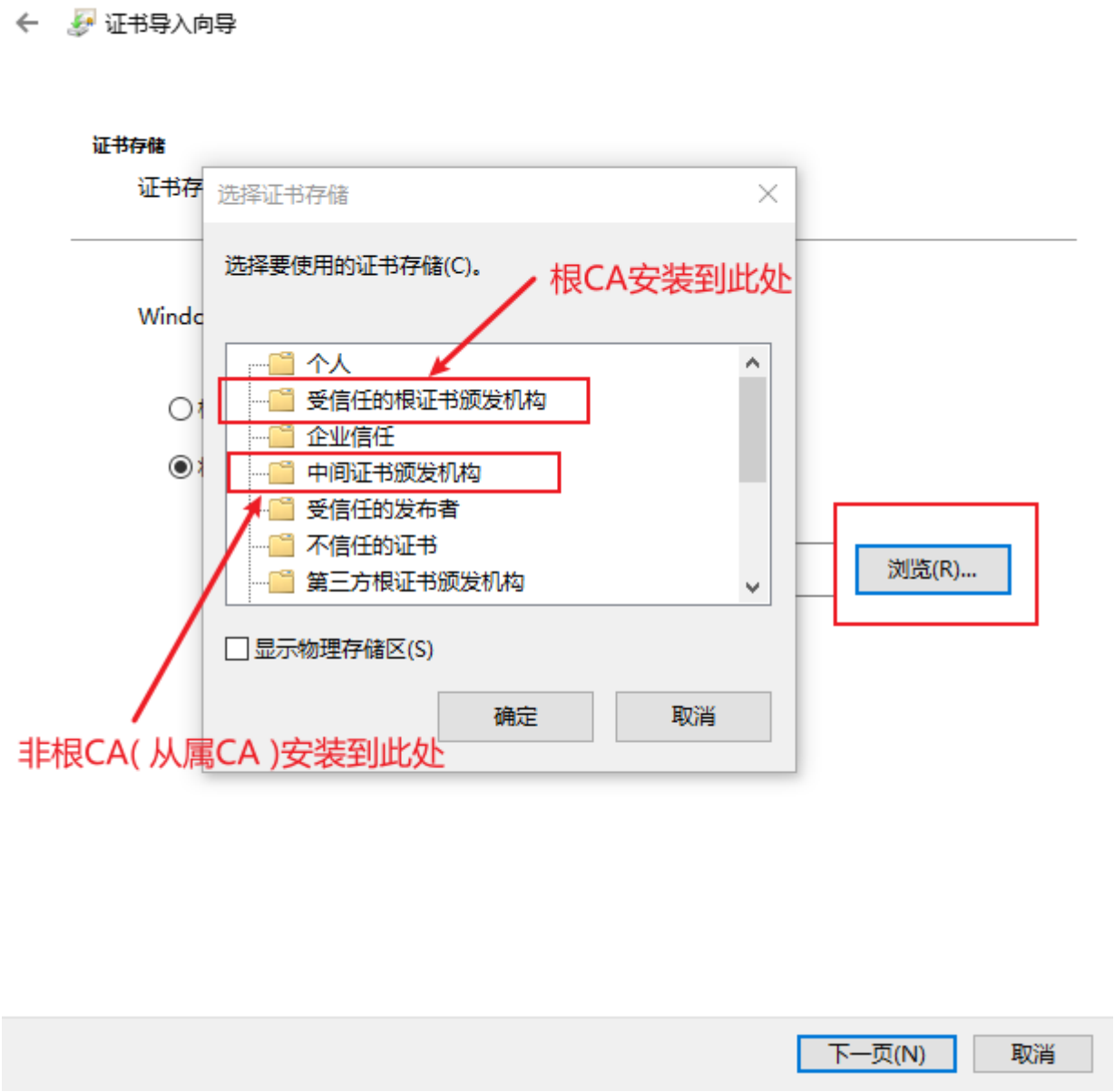


3. 存储位置选择 `当前用户` ，单击 `下一页` 。

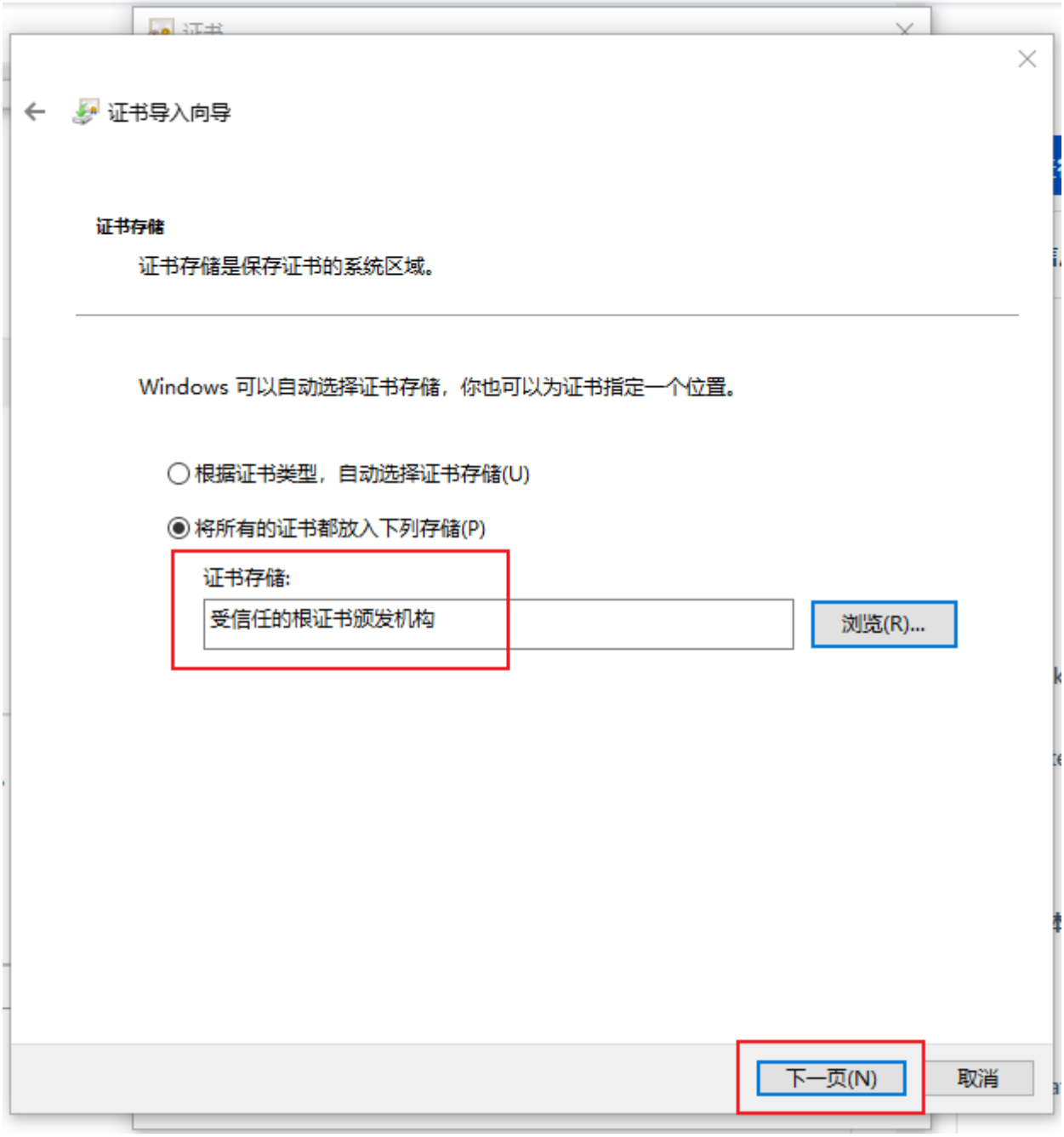
4. 选择 `将所有的证书都放入下列存储(P)` 。



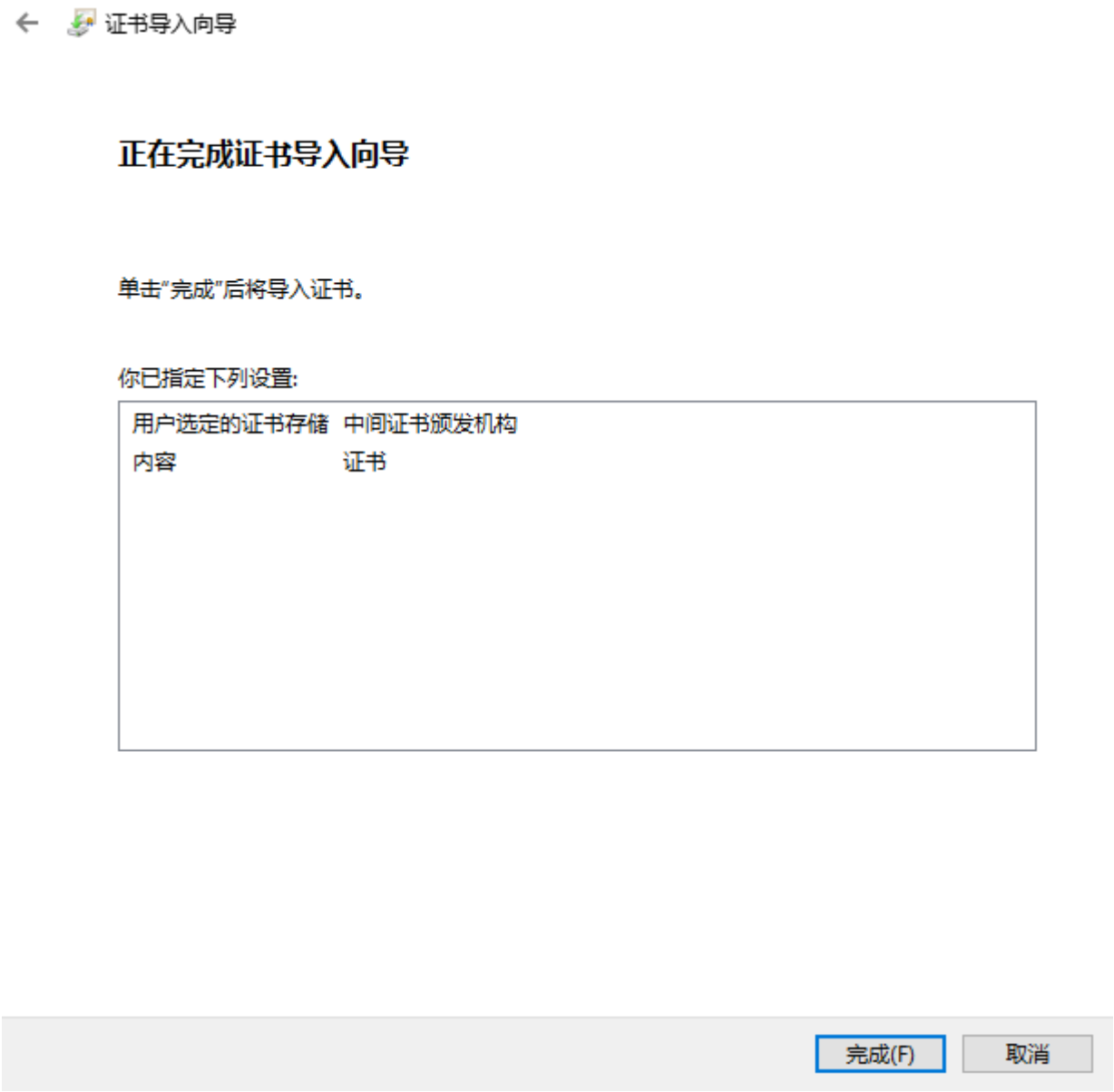
5. 单击 `浏览` ，如果是根CA选择 `受信任的根证书颁发机构` ，如果是从属CA选择 `中间证书颁发机构` 。选择完成后单击 `确定` 。


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

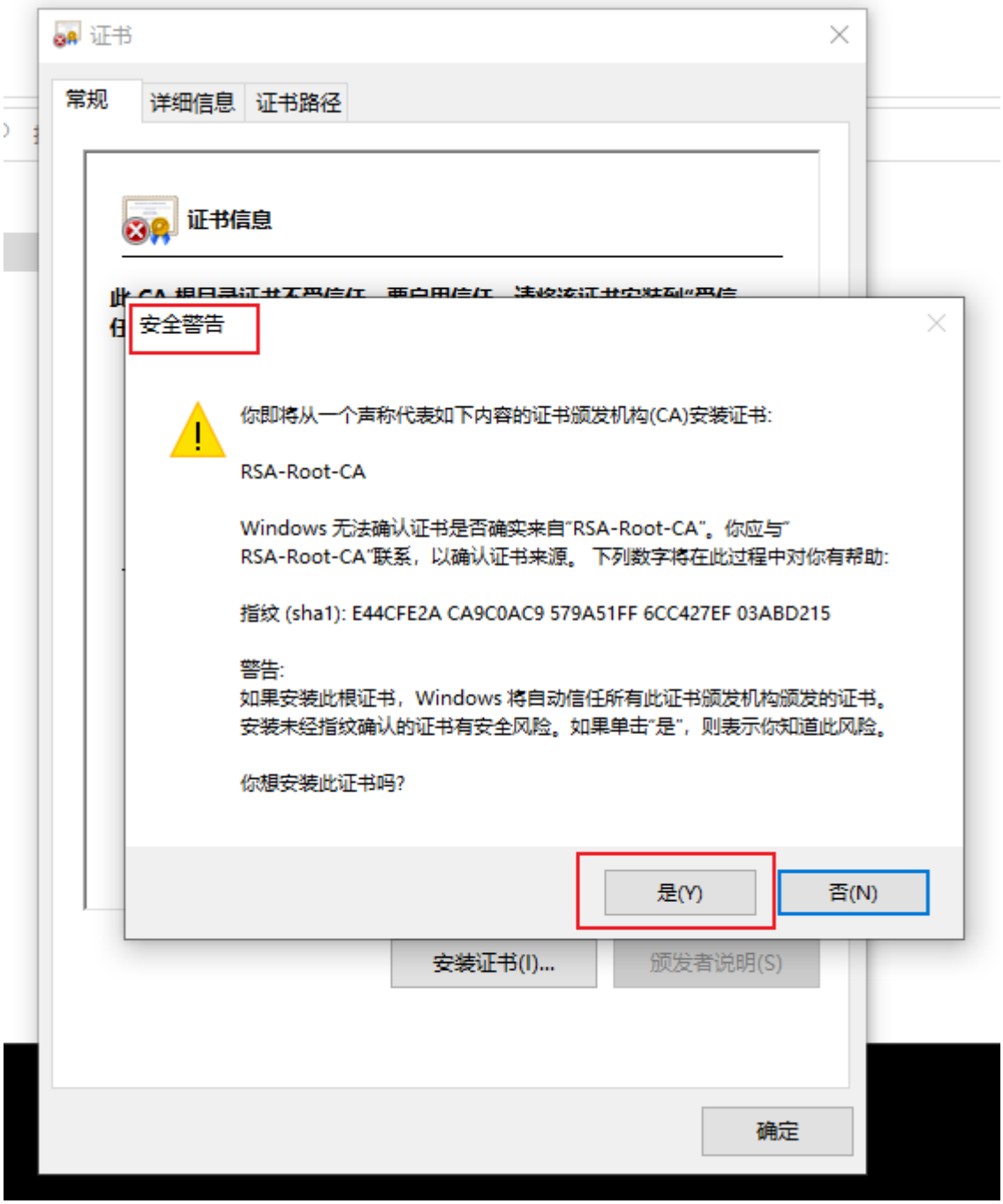
6. 单击 `下一页` 。

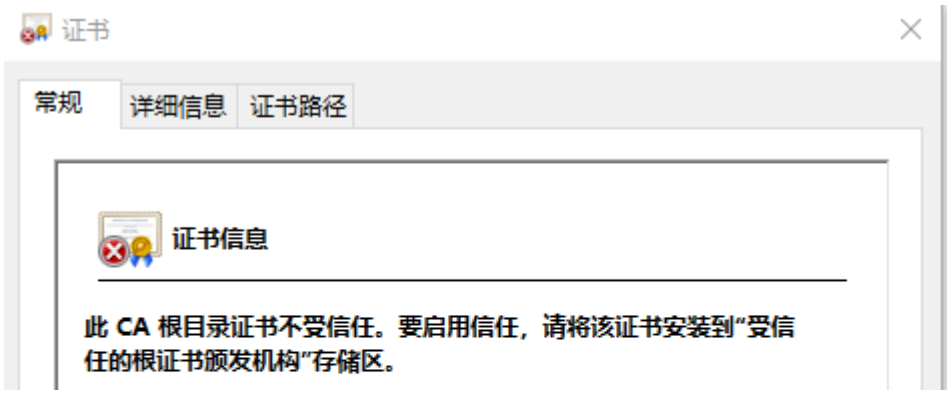


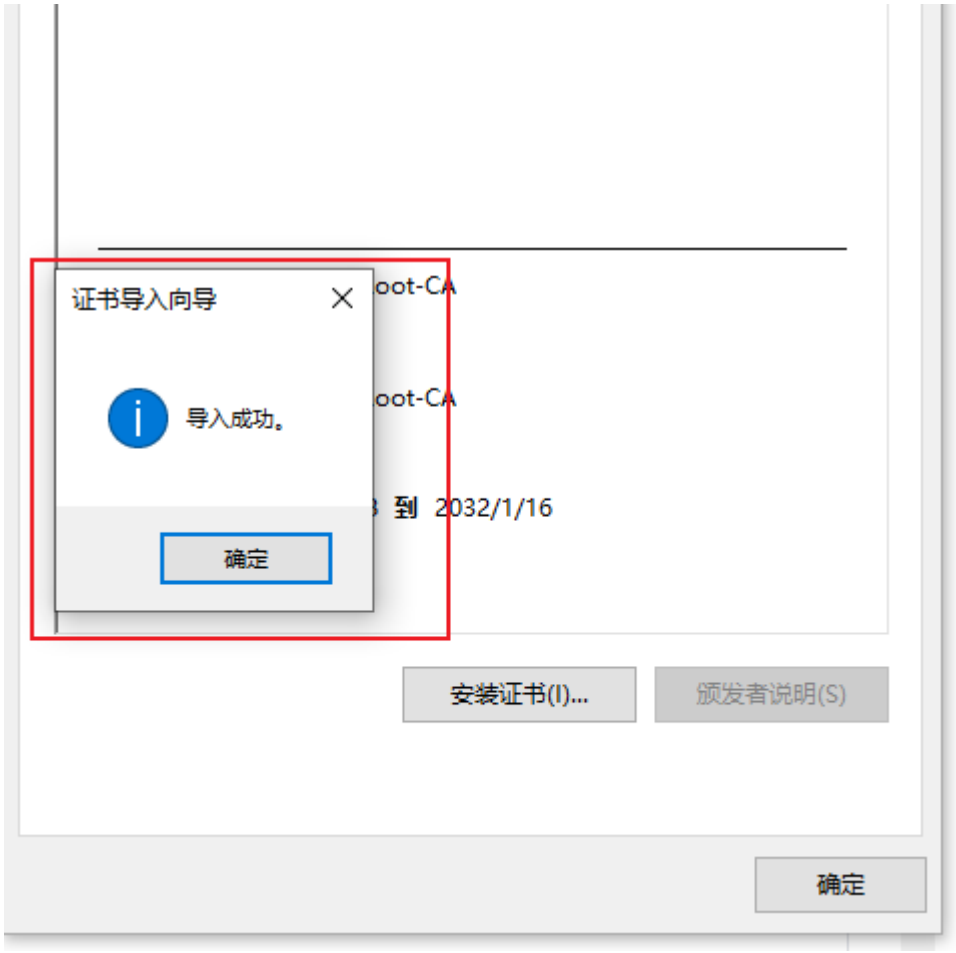
7. 单击 `完成` ，弹出安全警告窗口。


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。



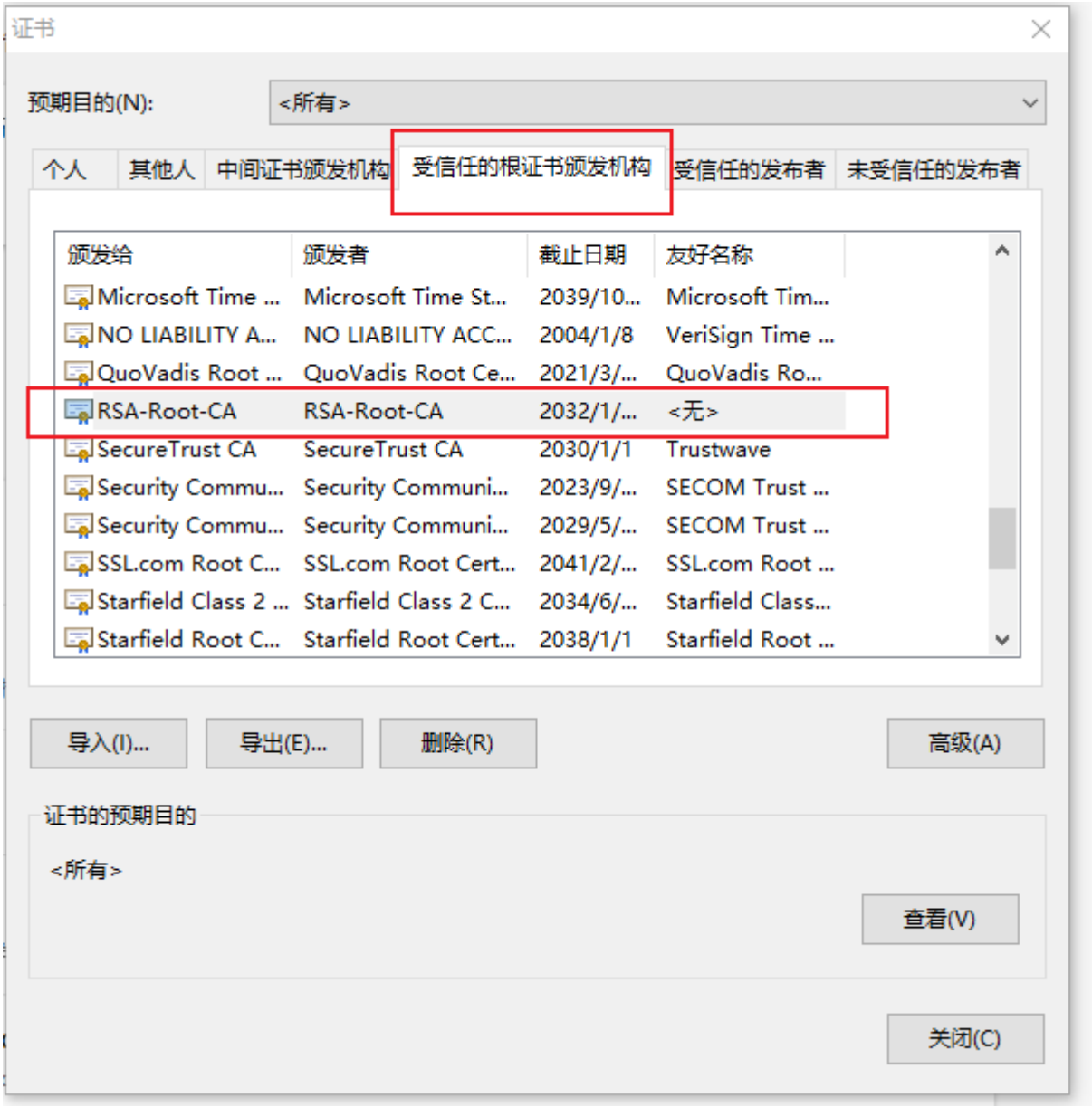
9. 重复以上步骤，依次安装该私有证书的签发CA到根CA的所有CA证书。

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。

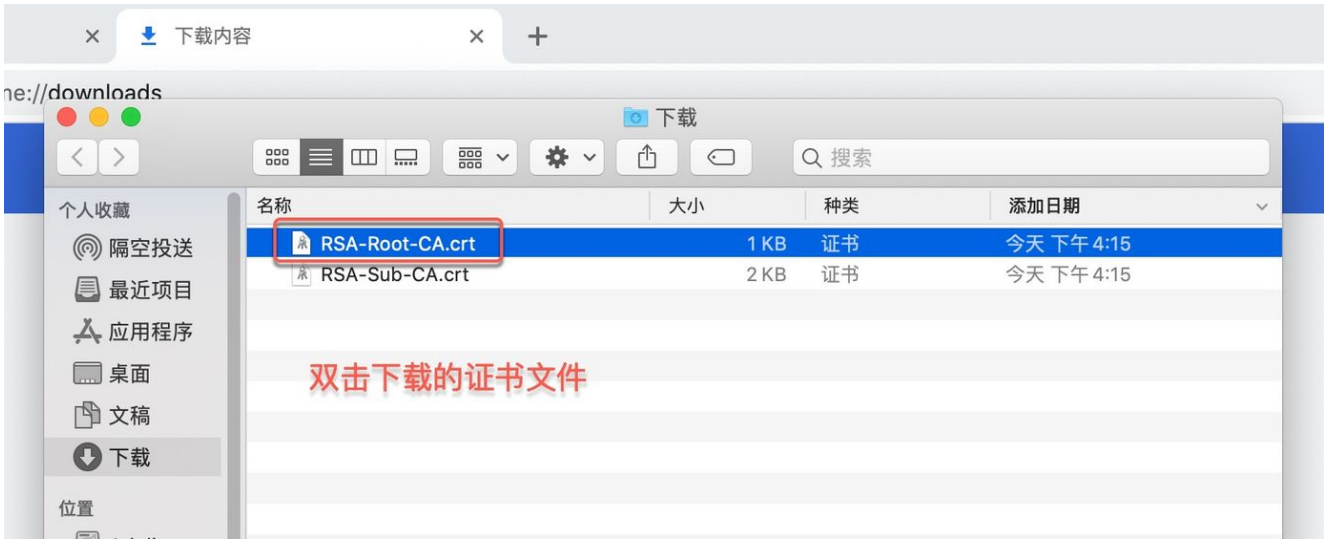


macOS操作系统

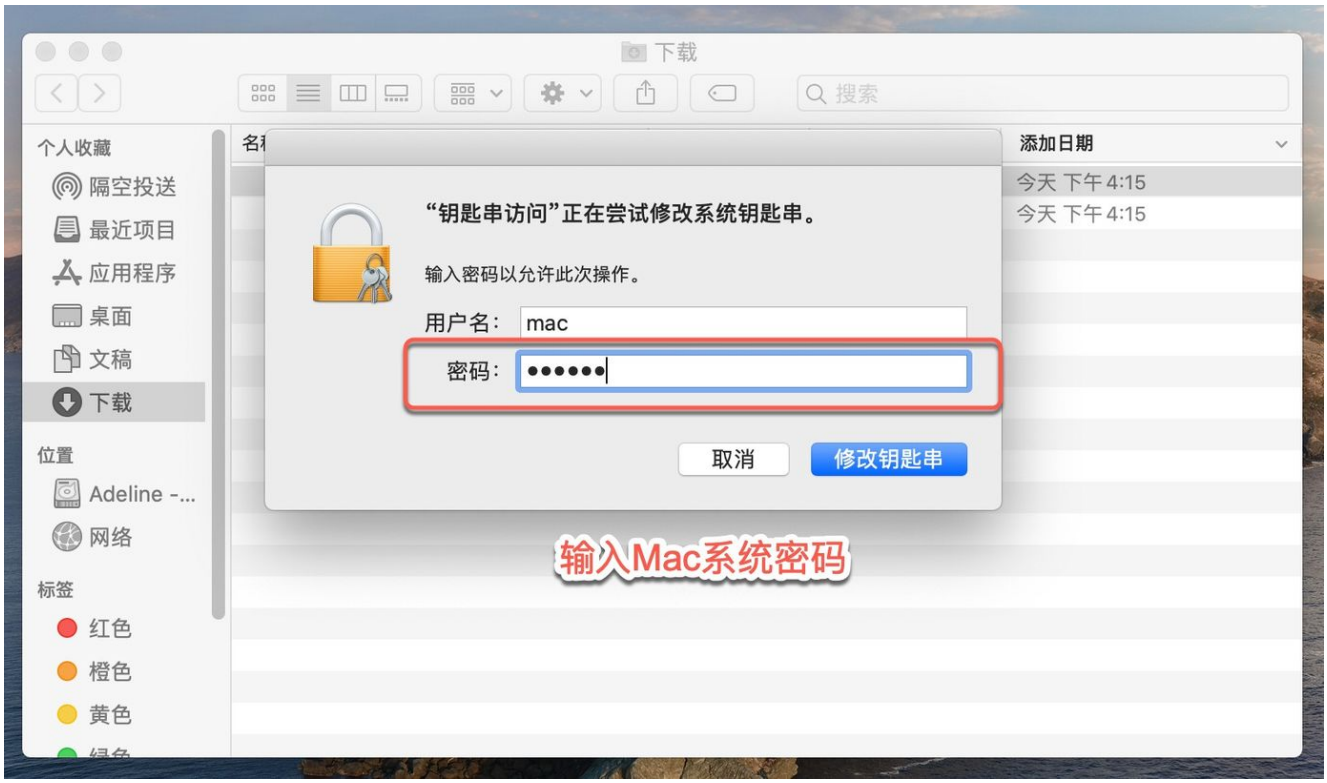
本节介绍在macOS操作系统中，如何导入私有证书的签发CA证书链，使其成为受信任的证书颁发机构。

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。

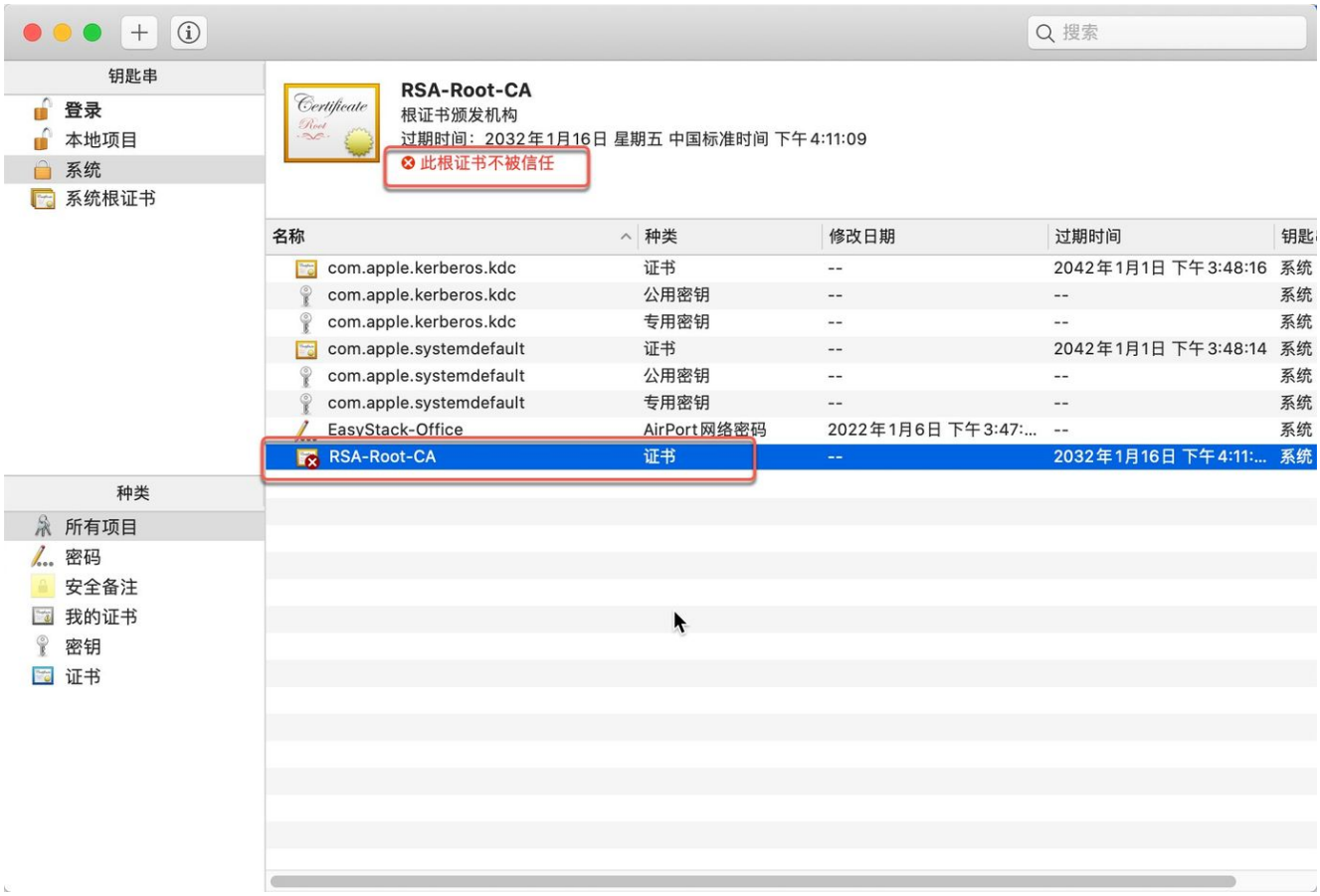
2. 双击某个证书文件，弹出密码输入窗口。



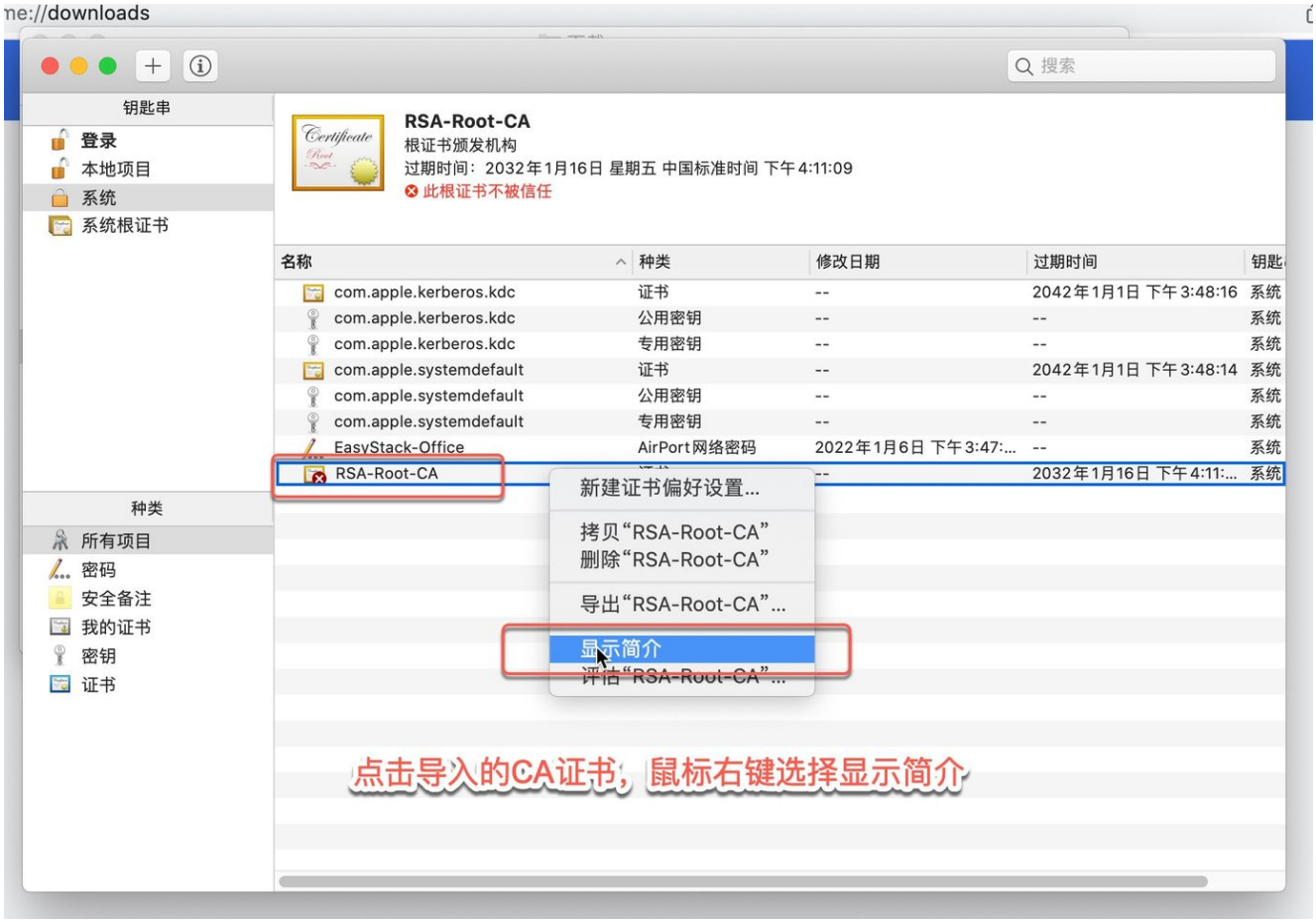
3. 输入系统密码，单击 修改钥匙串 ，弹出钥匙串列表。



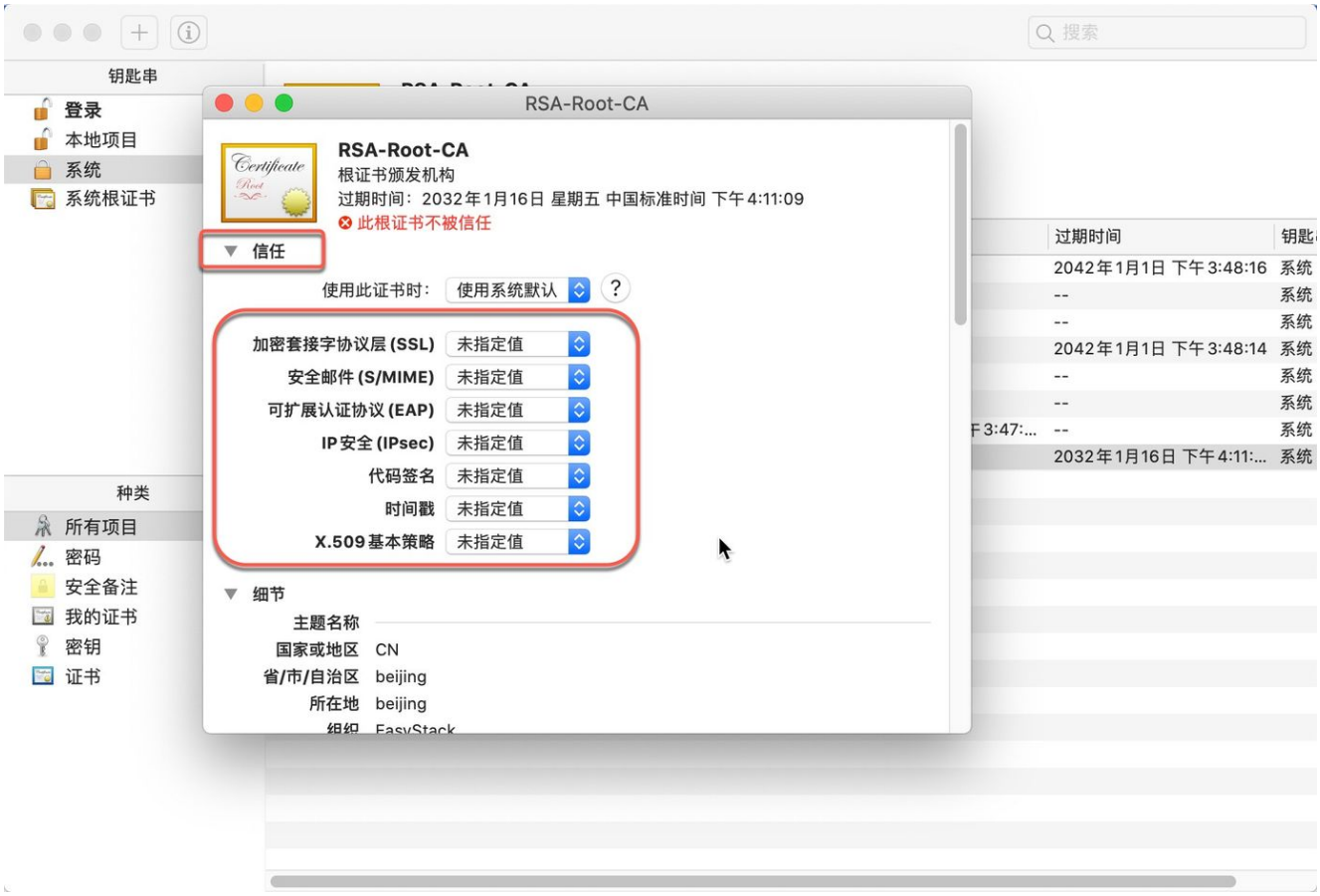
4. 此时虽然私有CA的证书已经导入到系统钥匙串中，但仍不受系统信任。



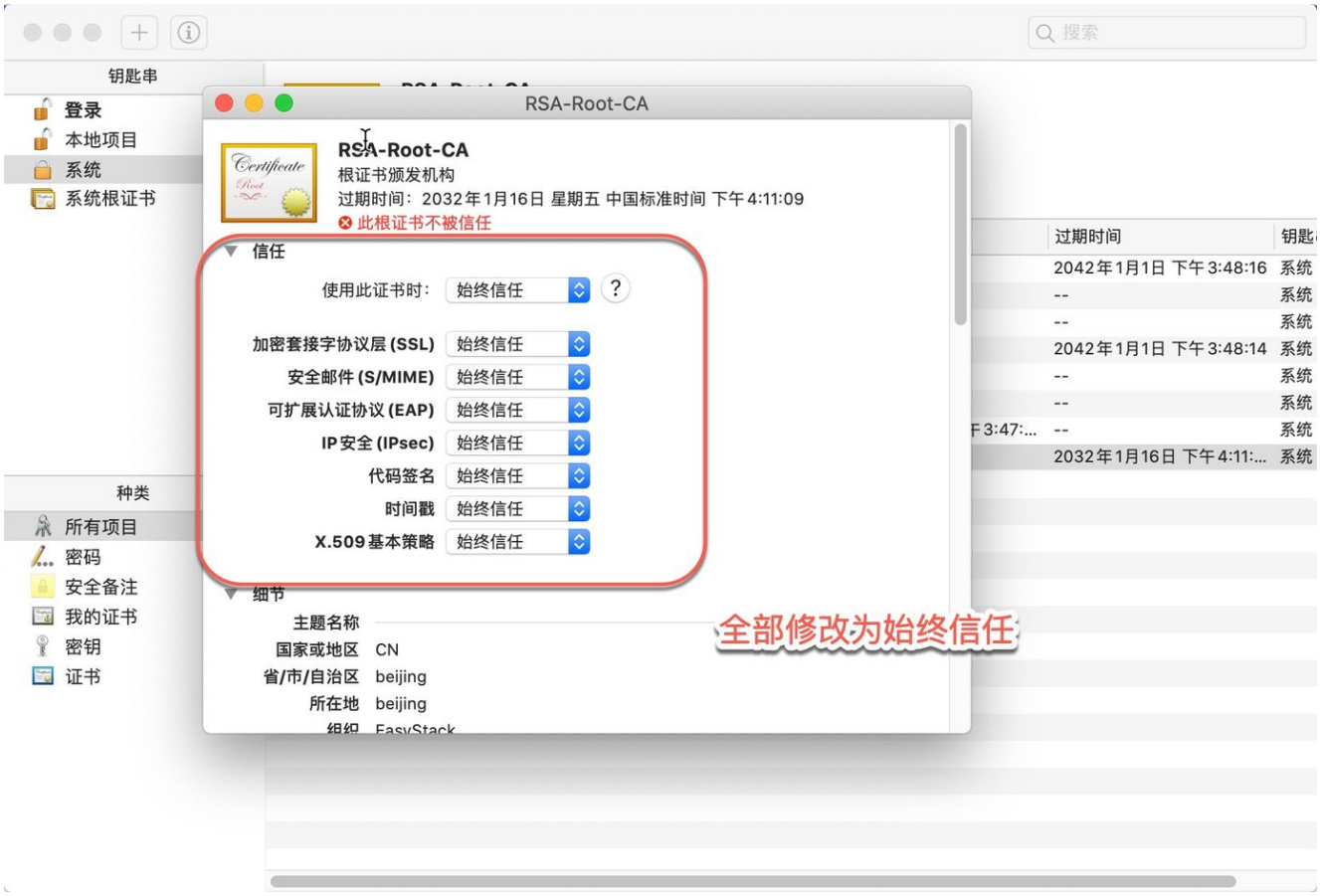
5. 右键单击导入的私有CA证书，选择“显示简介”。



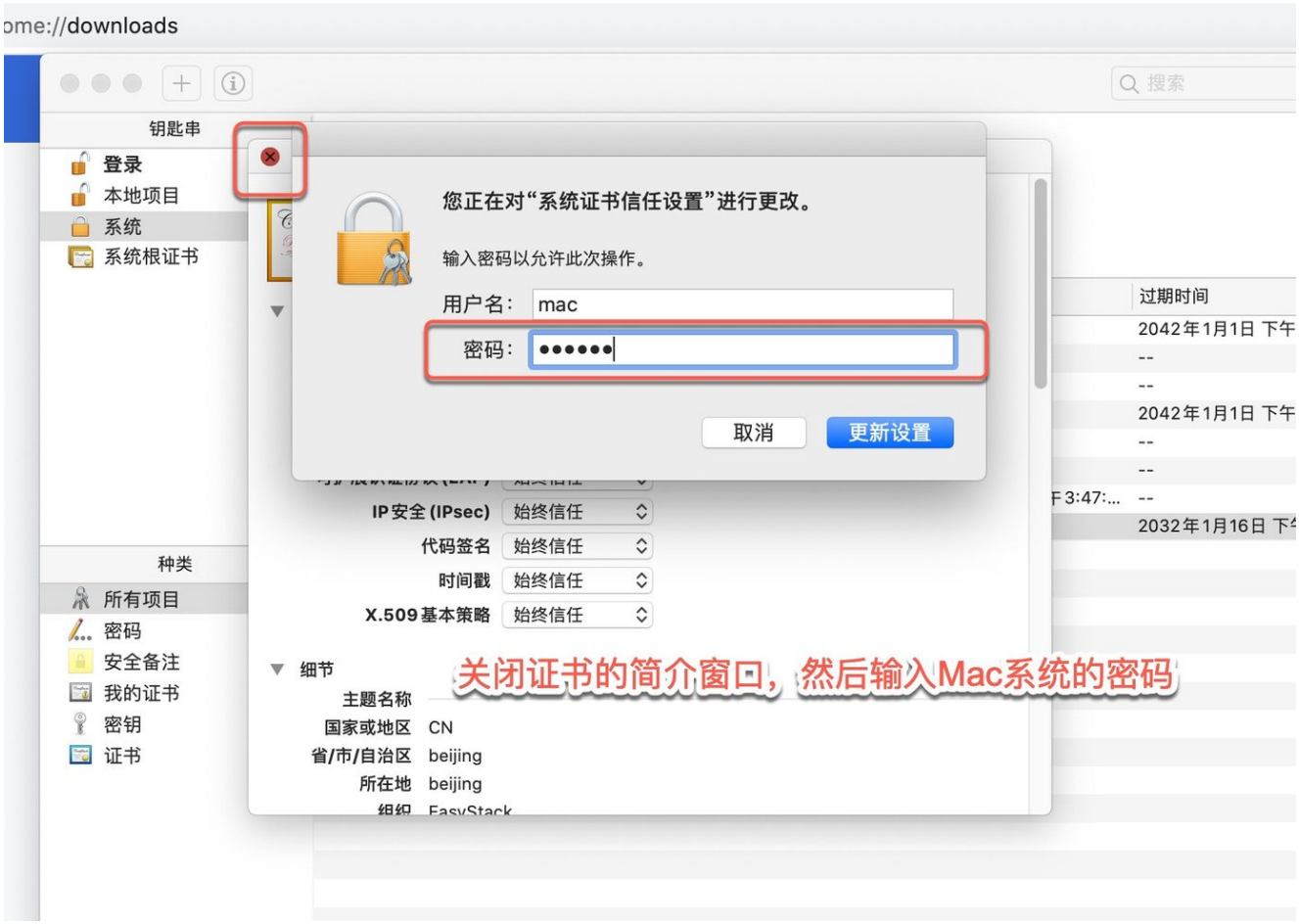
6. 展开“信任”下的详细信息。



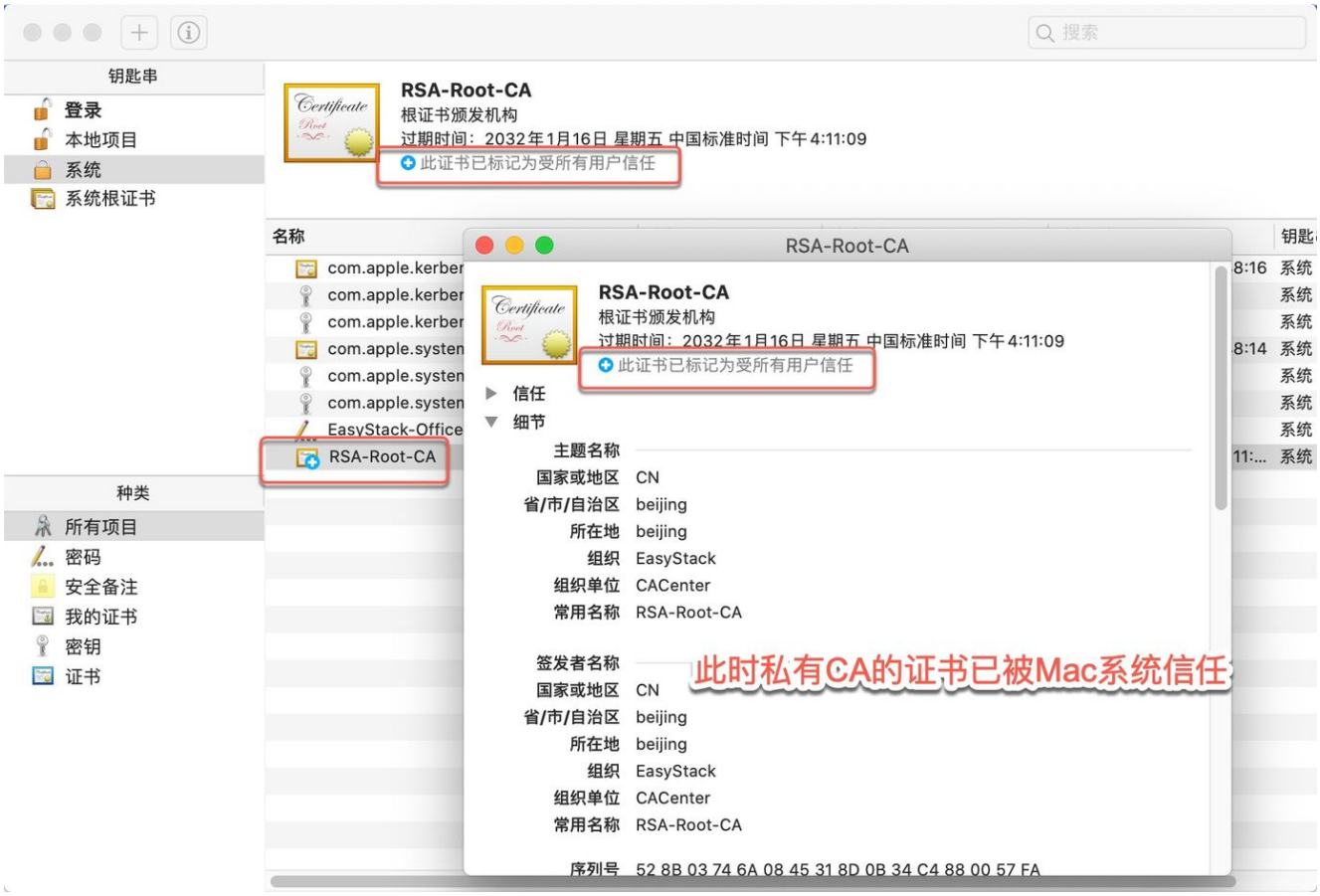
7. 将详细信息中的所有选项改为“始终信任”。



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。



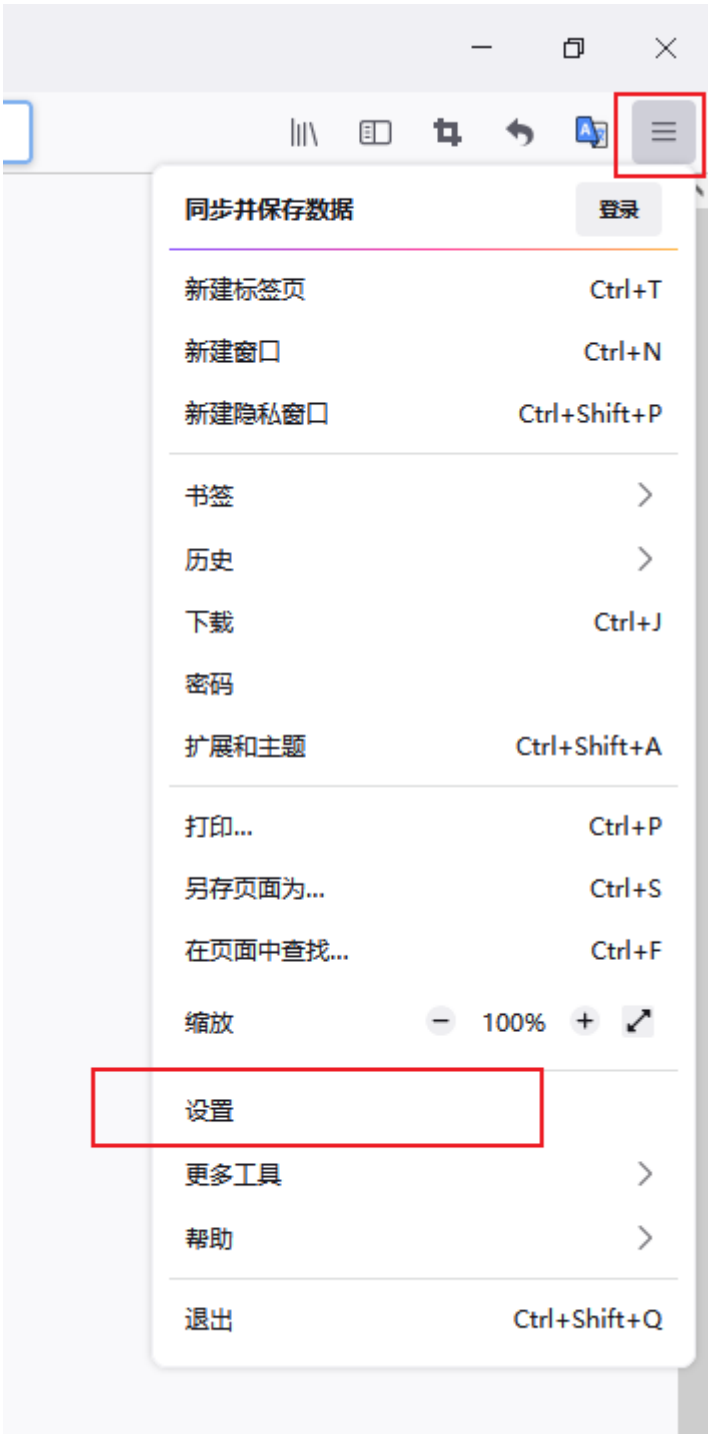
9. 再次在钥匙串列表中查看导入的私有CA证书，已被系统信任。



Firefox浏览器

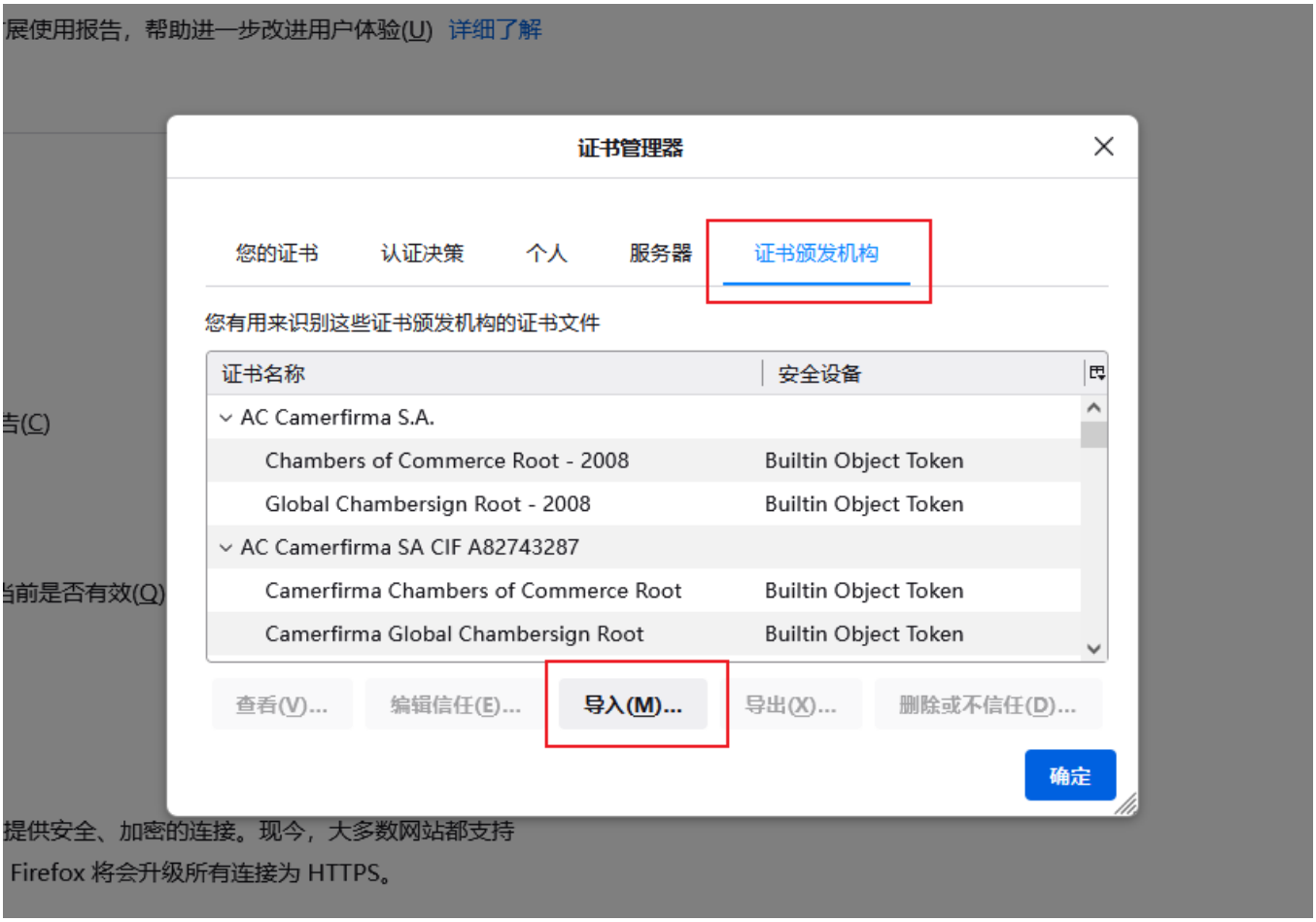
本节介绍如何在Firefox浏览器中导入私有证书的签发CA证书链，使其成为受信任的证书颁发机构。

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。

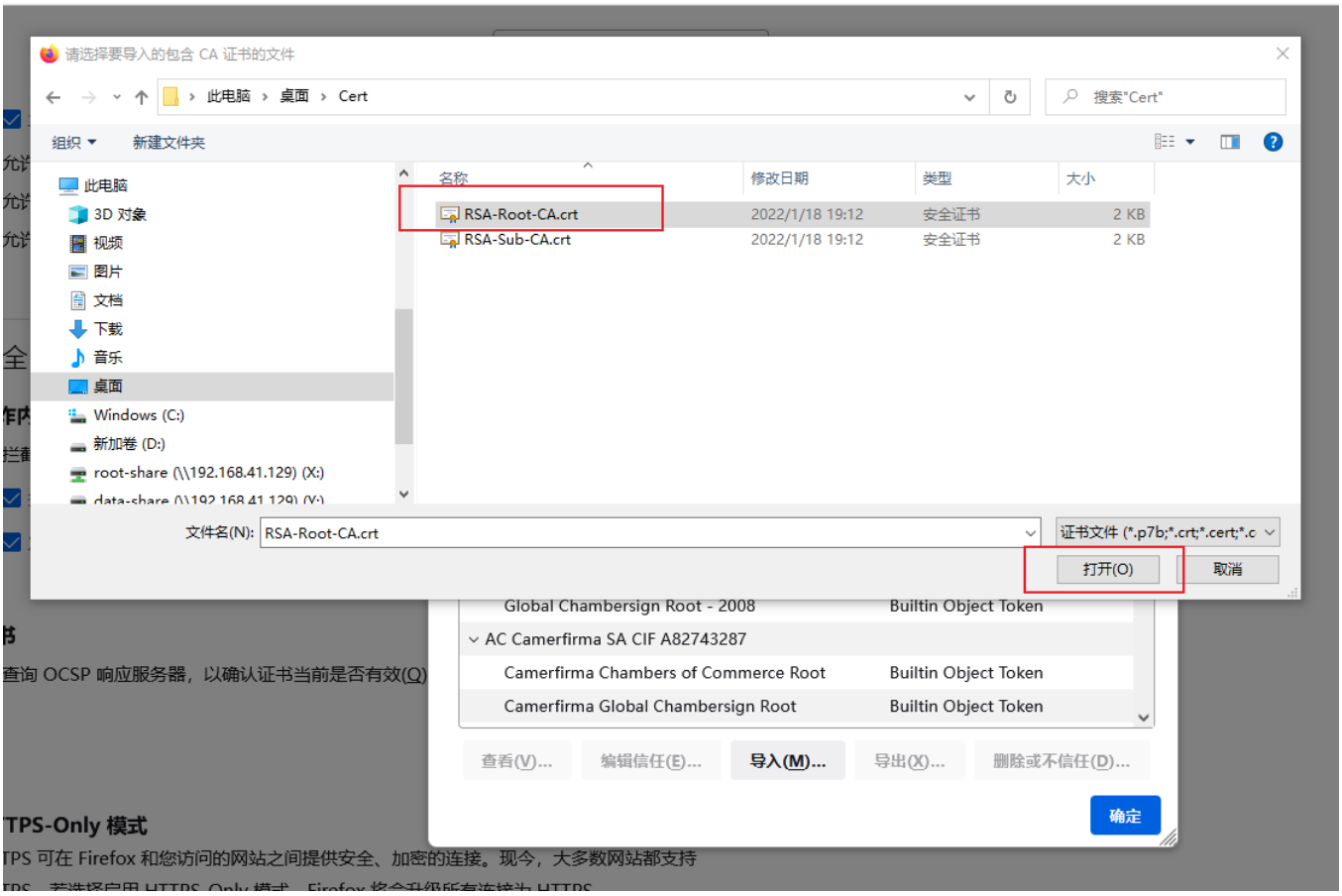


3. 在“隐私与安全”菜单项中，找到“证书”，单击 查看证书 。

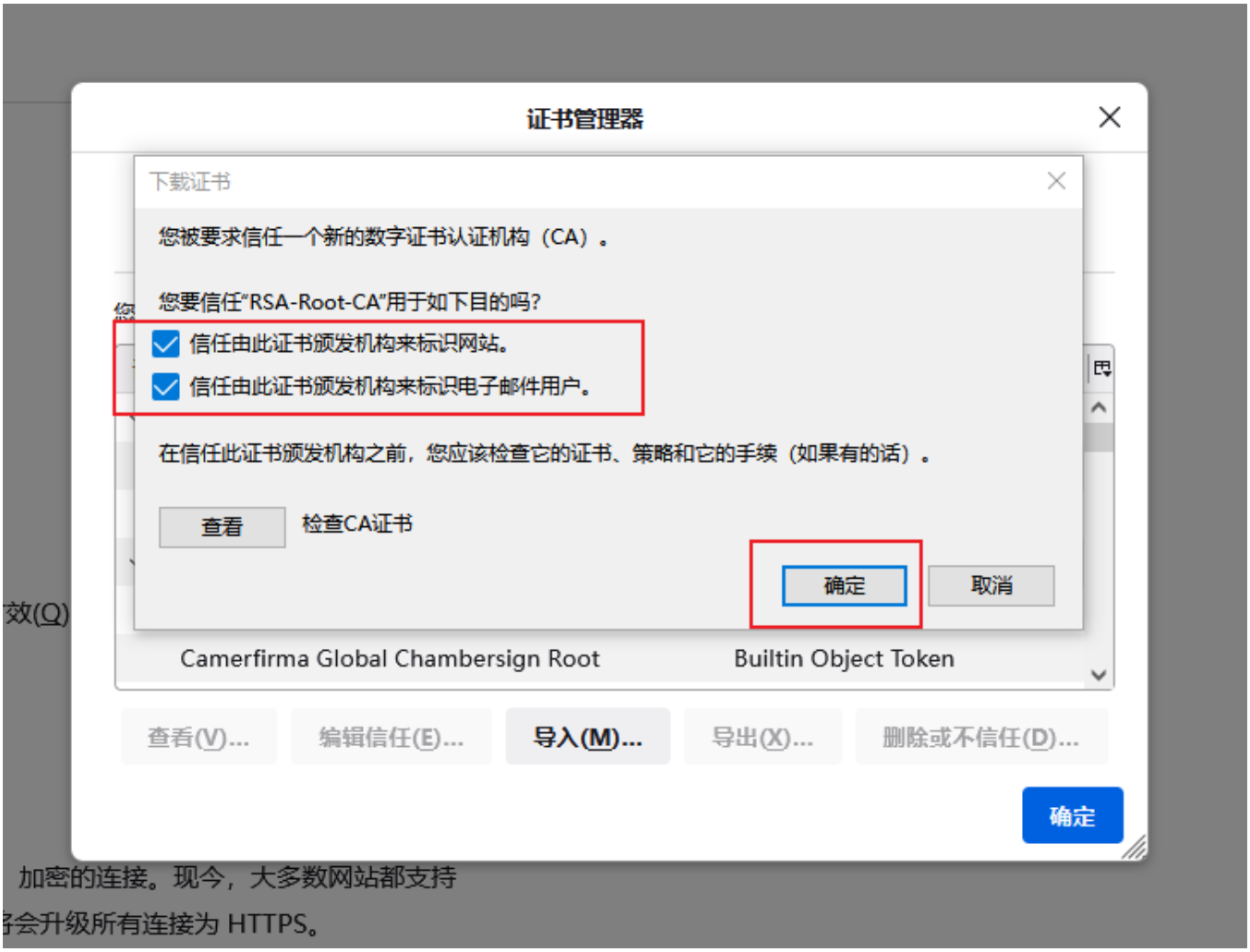
4. 在弹出的证书管理器中，选择“证书颁发机构”页签，单击 `导入` 。



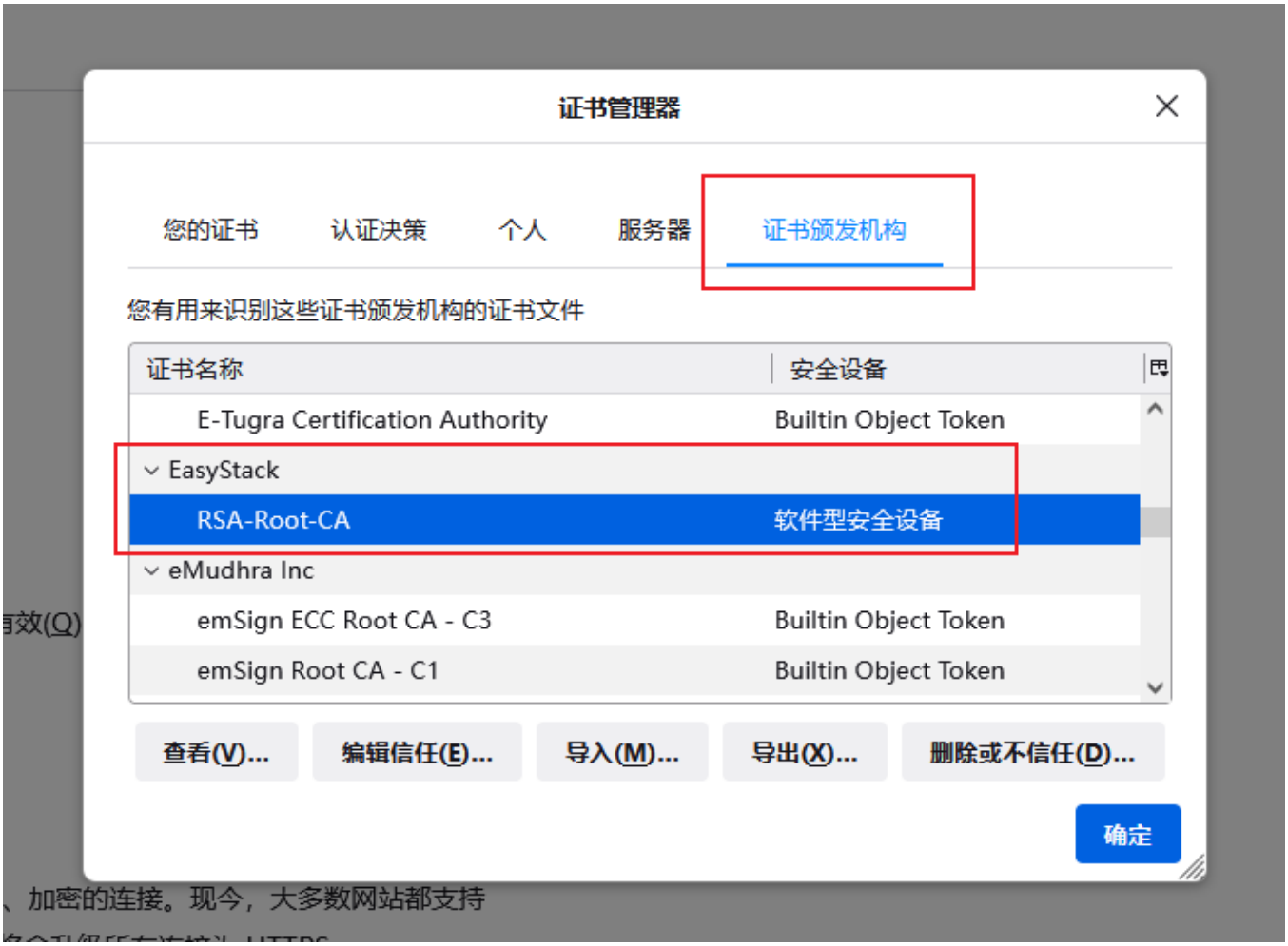
5. 选择下载好的私有CA证书文件，单击 `打开` 。



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。

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。

5.3 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。

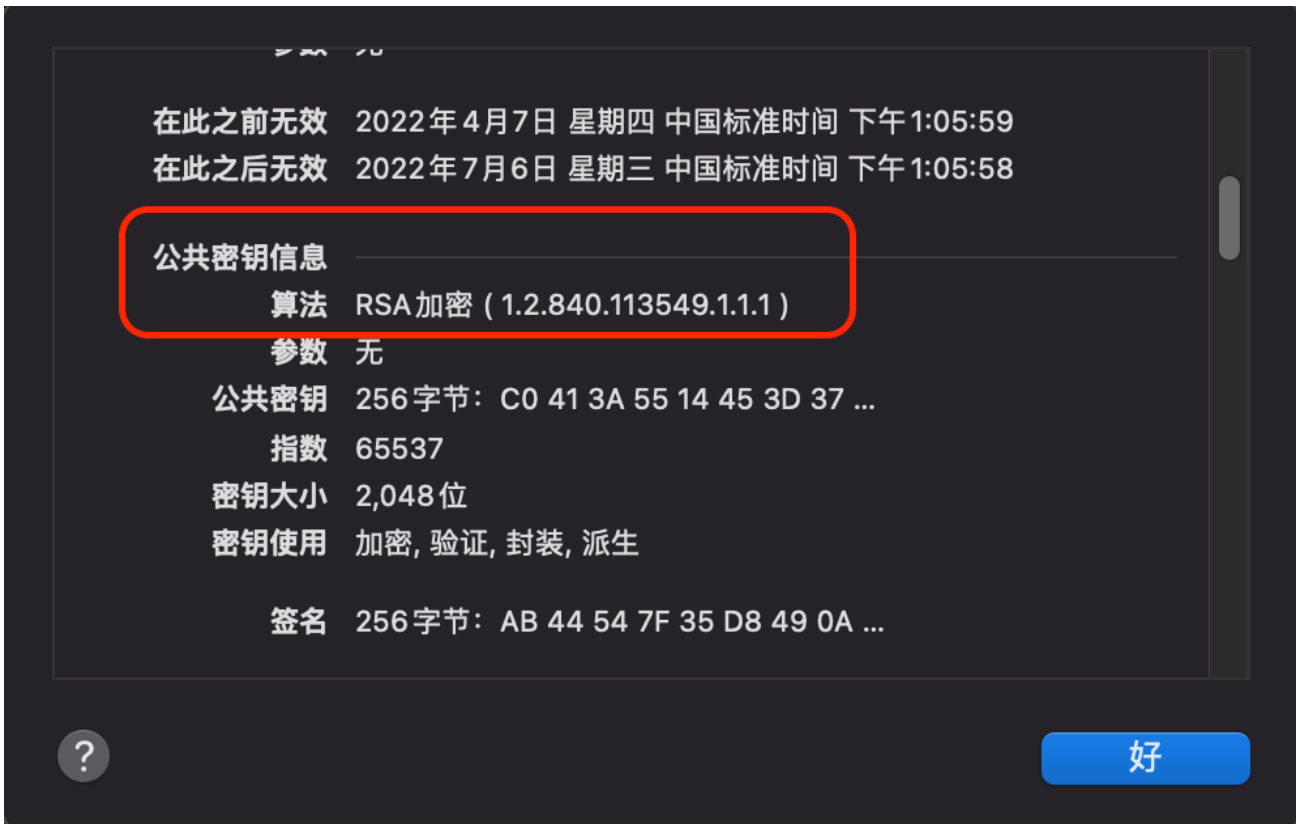
所以，当所上传证书的私钥格式为通用PEM格式时，需要手动将其转换为对应算法的私钥。

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>
```

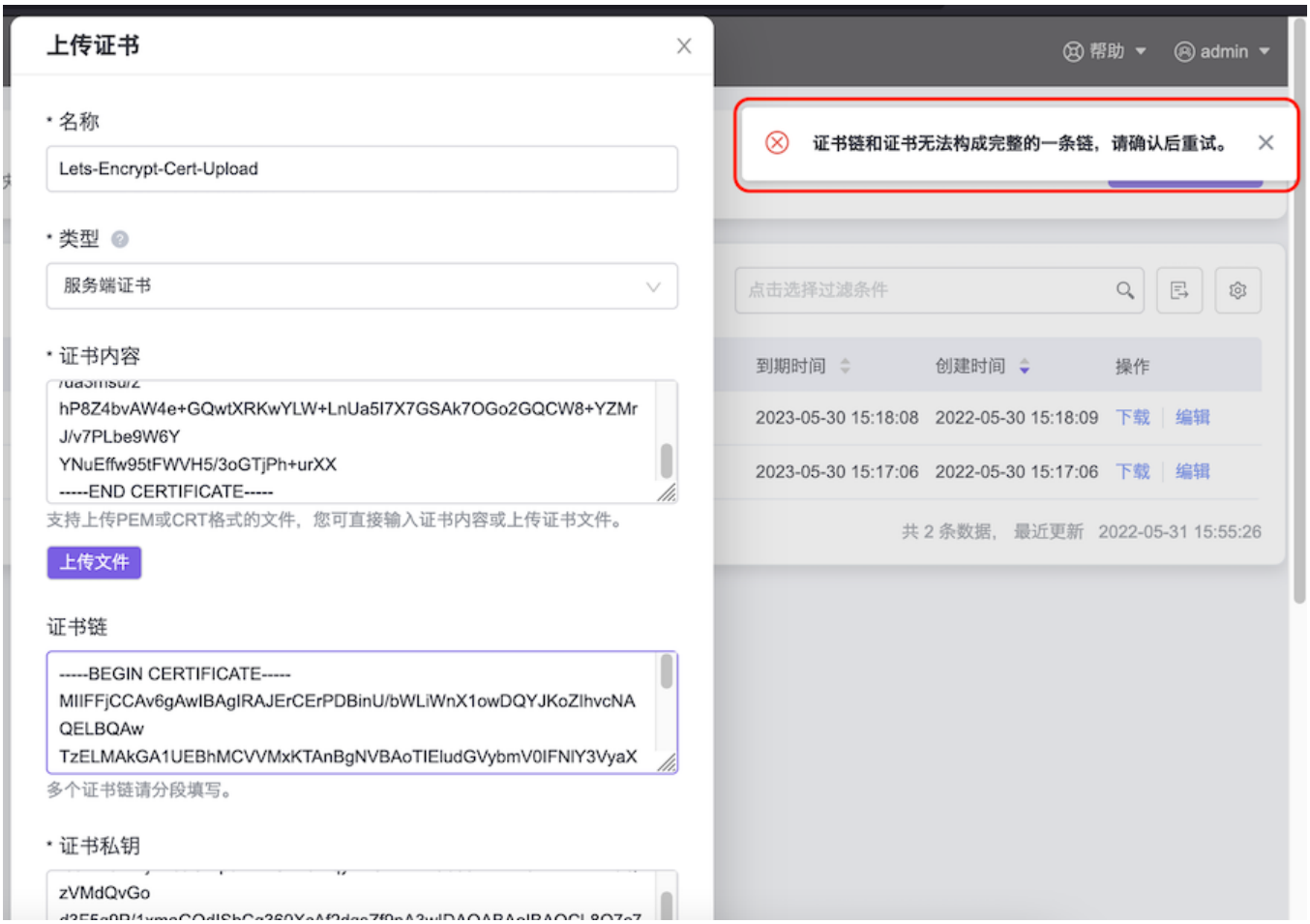
参数	说明
私钥算法	证书对应私钥的算法，即上一步骤中所获取到的算法。 当算法类型为RSA时，该参数值为 **rsa**。当算法类型为ECC时，该参数值为 **ec**。
通用格式私钥文件路径	转换前证书私钥文件的路径。

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。

5.4 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。

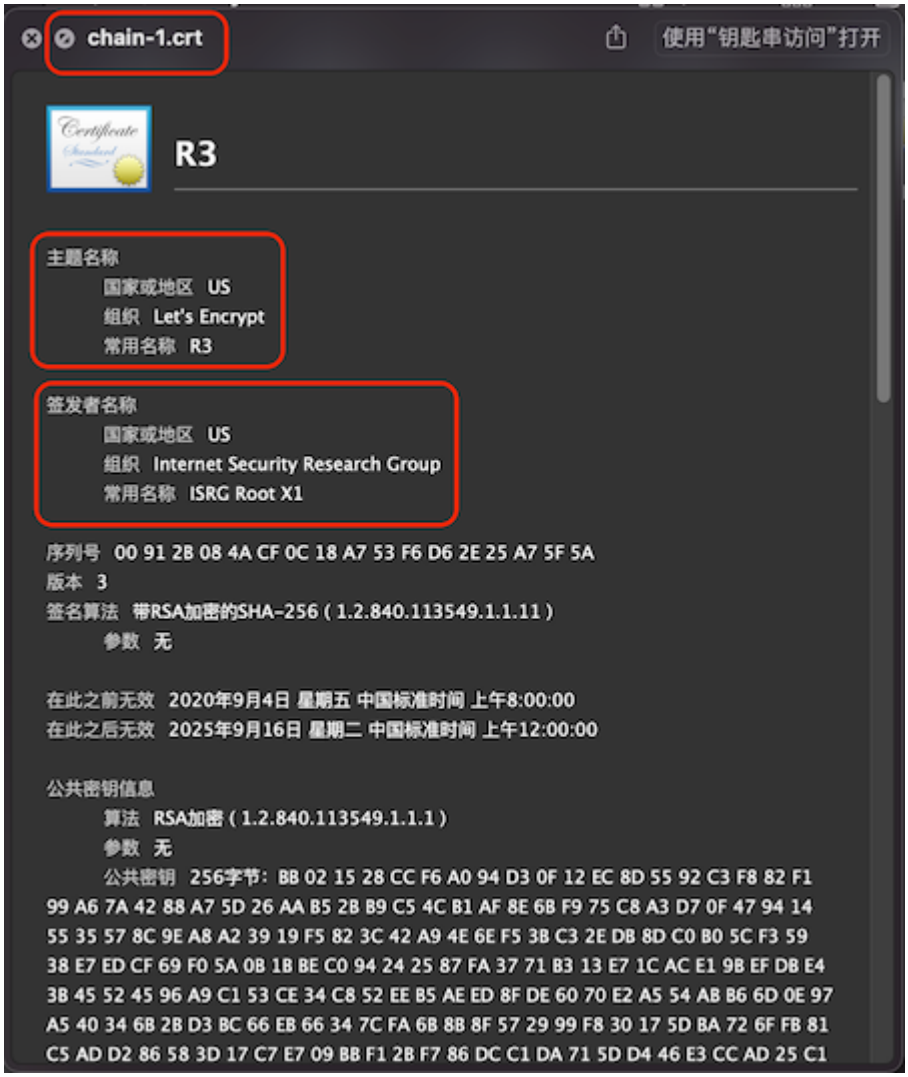
解决方案

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：

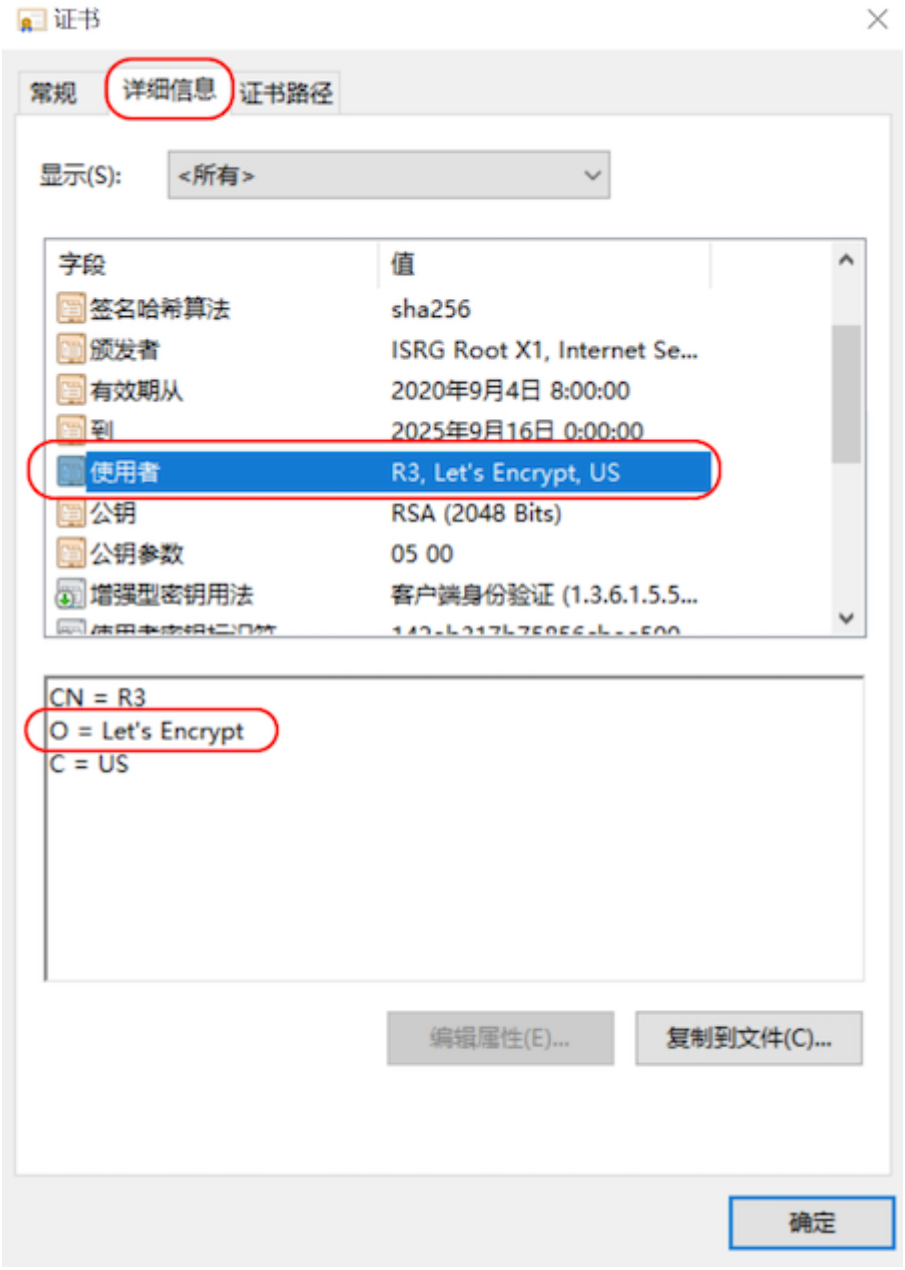
   - Mac操作系统：

     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。

6 API参考

6.1 API简介

欢迎使用API文档，如果您熟悉CA以及证书体系和一种以上编程语言，推荐您调用API管理您的资源和开发自己的应用程序。 本文档提供了API的描述、语法、参数说明及示例等内容。在调用API之前，请确保已经充分了解相关术语，详细信息请参见下表。

术语	说明
CA	证书授权中心（Certificate Authority）或称证书授权机构。
证书	证书又称终端实体证书，安装在终端实体上的证书，含客户端证书（应用于客户端）、服务器证书（应用于服务器）等。承担实体的身份验证的作用，不可用于签发证书，属于证书链中的最后一层，是拥有该证书的实体与其它实体进行HTTPS通信的凭证。
证书链	从根CA到终端实体证书之间的完整的证书链路，即各个层级证书按序链在一起的文件，用于进行身份的逐层校验。
HTTPS	HTTPS也就是HTTP+SSL，基于SSL协议的网站加密传输协议，是HTTP的安全版。

6.2 调用方式

请求结构

API支持基于URI发起HTTP/HTTPS GET请求。请求参数需要包含在URI中。本文列举了GET请求中的结构解释，并以云主机的服务接入地址为例进行了说明。

结构示例

以下为一条未编码的URI请求示例： `http://cloud.com/v1/{project_id}/servers` 在本示例中：

- `http` 指定了请求通信协议
- `cloud.com` 指定了服务接入地址
- `/v1/{project_id}/servers` 为资源路径，也即API访问路径

通信协议

支持HTTP或HTTPS协议请求通信。为了获得更高的安全性，推荐您使用HTTPS协议发送请求。涉及敏感数据时，如用户密码和SSH密钥对，推荐使用HTTPS协议。

服务网址

调用本文档所列举的API时均需使用OpenStack身份服务进行身份验证。 他们还需要一个从“compute”类型的标识符提取出来的“service URI”。 这将是根URI，将添加下面的每个调用来构建一个完整的路径。例如，如果“service URI”是 `http://mycompute.pvt/compute/v2.1` ，那么“/servers”的完整API调用是 `http://mycompute.pvt/compute/v2.1/servers` 。 根据部署计算服务网址可能是http或https，自定义端口，自定义路径，并包含您的租户ID。 要知道您的部署网址的唯一方法是通过使用服务目录。计算URI不应该被硬编码在应用程序中，即使他们只希望在单一地点工作。应始终从身份令牌中发现。因此，对于本文件的其余部分，我们将使用短针，其中"GET /servers"的真正含义"GET your_compute_service_URI/servers"。

请求方法

HTTP请求方法（也称为操作或动词），它告诉服务你正在请求什么类型的操作。

方法	说明

方法	说明
GET	从服务端读取指定资源的所有信息，包括数据内容和元数据（Metadata）信息，其中元数据在响应头（Response Header）中返回，数据内容在响应体（Response Body）中。
PUT	向指定的资源上传数据内容和元数据信息。如果资源已经存在，那么新上传的数据将覆盖之前的内容。
POST	向指定的资源上传数据内容。与PUT操作相比，POST的主要区别在于POST一般用来向原有的资源添加信息，而不是替换原有的内容：POST所指的资源一般是处理请求的服务，或是能够处理多块数据。
DELETE	请求服务器删除指定资源，如删除对象等。
HEAD	仅从服务端读取指定资源的元数据信息。

字符编码

请求及返回结果都使用UTF-8字符集编码。

公共参数

公共参数是用于标识用户和接口签名的参数，如非必要，在每个接口单独的接口文档中不再对这些参数进行说明，但每次请求均需要携带这些参数，才能正常发起请求。

公共请求参数

名称	类型	是否必选	描述
Host	String	否（使用AK/SK认证时该字段必选）	请求的服务器信息，从服务API的URI中获取。值为hostname[:port]。端口缺省时使用默认的端口，https的默认端口为443。

名称	类型	是否必选	描述
Content-Type	String	是	消息体的类型（格式）。推荐用户使用默认值application/json，有其他取值时会在具体接口中专门说明。
Content-Length	String	否	请求body长度，单位为Byte。
X-Project-Id	String	否	project id，项目编号。
X-Auth-Token	String	否（使用Token认证时该字段必选）	用户Token。用户Token也就是调用获取用户Token接口的响应值，该接口是唯一不需要认证的接口。请求响应成功后在响应消息头（Headers）中包含的“X-Subject-Token”的值即为Token值。

公共返回参数

参数名称	参数类型	描述
RequestId	String	请求ID。无论调用接口成功与否，都会返回该参数。

签名机制

调用接口的认证方式为Token认证，通过Token认证通用请求。 Token在计算机系统中代表令牌（临时）的意思，拥有Token就代表拥有某种权限。Token认证就是在调用API的时候将Token加到请求消息头，从而通过身份认证，获得操作API的权限。 Token可通过调用获取用户Token接口获取，调用本服务API需要project级别的Token，即调用获取用户Token接口时，请求body中 `auth.scope` 的取值需要选择 `project` ，如下所示：

```
{
    "auth": {
        "scope": {
            "project": {
                "domain": {
                    "name": "Default"
```

```
                },
                "name": "admin"
            }
        },
        "identity": {
            "password": {
                "user": {
                    "password": "devstacker",
                    "id": "858634b407e845f14b02bcf369225dcd0"
                }
            },
            "methods": ["password"]
        }
    }
}
```

获取Token后，再调用其他接口时，您需要在请求消息头中添加 `X-Auth-Token` ，其值即为 `Token` 。例如Token值为“ABCDEFJ....”，则调用接口时将 `X-Auth-Token: ABCDEFJ....` 加到请求消息头即可，如下所示:

```
POST https://iam.cn-north-1.mycloud.com/v3/auth/projects
Content-Type: application/json
X-Auth-Token: ABCDEFJ....
```

返回结果

请求发送以后，您会收到响应，包含状态码、响应消息头和消息体。 状态码是一组从1xx到5xx的数字代码，状态码表示了请求响应的状态。 为了便于查看和美观，API 文档返回示例均有换行和缩进等处理，实际返回结果无换行和缩进处理。

正确返回结果

接口调用成功后会返回接口返回参数和请求 ID，我们称这样的返回为正常返回。HTTP 状态码为 2xx。 以云主机的接口创建云主机 `(POST /v1/{project_id}/servers)` 为例，若调用成功，其可能的返回如下:

```
{
    "error": {
        "OS-DCF:diskConfig": "AUTO",
        "adminPass": "6NpUwoz2QDRN",
```

```
        "id": "f5dc173b-6804-445a-a6d8-c705dad5b5eb",
        "links": [
            {
                "href":
"http://openstack.example.com/v2/6f70656e737461636b20342065766572/servers/f5
dc173b-6804-445a-a6d8-c705dad5b5eb",
                "rel": "self"
            },
            {
                "href":
"http://openstack.example.com/6f70656e737461636b20342065766572/servers/f5dc1
73b-6804-445a-a6d8-c705dad5b5eb",
                "rel": "bookmark"
            }
        ],
        "security_groups": [
            {
                "name": "default"
            }
        ]
    }
}
```

错误返回结果

接口调用出错后，会返回错误码、错误信息和请求 ID，我们称这样的返回为异常返回。HTTP 状态码为 4xx 或者 5xx。

```
{
    "error": {
        "message": "The request you have made requires authentication.",
        "code": 401,
        "title": "Unauthorized"
    }
}
```

公共错误码

http状态码	Error Message	说明
300	multiple choices	被请求的资源存在多个可供选择的响应。
400	Bad Request	服务器未能处理请求。
401	Unauthorized	被请求的页面需要用户名和密码。
403	Forbidden	对被请求页面的访问被禁止。
404	Not Found	服务器无法找到被请求的页面。
405	Method Not Allowed	请求中指定的方法不被允许。
406	Not Acceptable	服务器生成的响应无法被客户端所接受。
407	Proxy Authentication Required	用户必须首先使用代理服务器进行验证，这样请求才会被处理。
408	Request Timeout	请求超出了服务器的等待时间。
409	Conflict	由于冲突，请求无法被完成。
500	Internal Server Error	请求未完成。服务异常。
501	Not Implemented	请求未完成。服务器不支持所请求的功能。
502	Bad Gateway	请求未完成。服务器从上游服务器收到一个无效的响应。
503	Service Unavailable	请求未完成。系统暂时异常。
504	Gateway Timeout	网关超时。

6.3 证书管理

证书管理

列举证书

功能介绍

获取证书列表。

URI

`GET /v1/secrets`

请求消息

参数	参数类型	是否必选	描述
show_all	string	否	值为 `True` 时，返回所有项目下的证书资源；值为 `False` 时，返回当前项目下的证书资源。该参数仅在云管理员身份下有效。
show_expired	string	否	值为 `True` 时，返回的证书列表中将包含已经过期的证书。默认只返回未过期的证书。
show_cert_secrets_only	string	否	值为 `True` 时，仅返回证书类型的Secret资源。默认将返回所有类型的Secret资源。
use_es_deleted	string	否	值为 `True` 时，代表使用 `es_deleted` 字段标记证书是否被删除，防止负载均衡监听器引用已被删除的证书时报错。

参数	参数类型	是否必选	描述
cert_use_type	integer	否	值为 `1` 时，仅返回服务端证书；值为 `2` 时，仅返回客户端证书；默认返回所有类型的证书。
key_algorithm	integer	否	值为 `1` 时，仅返回 `RSA` 密钥算法类型的证书；值为 `2` 时，仅返回 `ECC` 密钥算法类型的证书；值为 `3` 时，仅返回国密SM2算法类型的证书；默认返回所有算法类型的证书。
limit	integer	否	返回的证书列表数据条数，默认返回10条数据，最大支持100条数据。
offset	integer	否	获取证书数据时的起始索引位置，即偏移量。一般结合 `limit` 参数一起使用。

响应消息

参数	参数类型	描述
name	string	Secret 资源名称，在证书服务中代表证书名称。
status	string	Secret 资源状态，证书服务中未使用此字段。
created	string	证书 Secret 创建时间。
updated	string	证书 Secret 更新时间。
secret_type	string	Secret 资源类型，证书服务中未使用此字段。
expiration	string	证书过期时间。
algorithm	string	Secret 资源加密算法类型，证书服务中未使用此字段。
bit_length	integer	Secret 资源加密算法位数，证书服务中未使用此字段。
mode	string	Secret 资源加密模式，证书服务中未使用此字段。

参数	参数类型	描述
creator_id	uuid	创建证书的用户ID。
es_dns	string	证书所绑定的域名信息。
es_cert_type	integer	证书状态， `1` 代表 `已签发` ； `2` 代表 `已托管` ； `3` 代表 `其他` ，用于标记非证书Secret资源； `4` 代表 `已吊销` 。
es_project_id	uuid	当前证书所处的项目ID。
es_domain_id	uuid	当前证书所处的部门ID。
es_issuer_ca_id	uuid	签发证书的私有CA的ID。
es_deleted	boolean	证书是否已删除。
es_cert_use_type	integer	证书类型， `1` 代表服务端证书， `2` 代表客户端证书。
es_key_algorithm	integer	证书密钥算法类型， `1` 代表RSA密钥算法， `2` 代表ECC密钥算法， `3` 代表国密SM2算法。
content_types	object	Secret对应的Payload内容格式类型。
secret_ref	string	证书资源对应的Secret引用，包含Secret ID。

请求示例

```
curl -X GET -H "X-Auth-Token: "
http://barbican.barbican.svc.cluster.local/v1/secrets?
show_all=True&show_cert_secrets_only=True&cert_use_type=1&use_es_deleted=Tru
e&key_algorithm=1
```

正常响应示例

```
{
    "secrets": [
        {
```

```
            "created": "2023-03-27T12:12:40",
            "updated": "2023-03-27T12:12:40",
            "status": "ACTIVE",
            "name": "server-cert-test",
            "secret_type": "opaque",
            "expiration": "2024-03-26T12:12:40",
            "algorithm": null,
            "bit_length": null,
            "mode": null,
            "creator_id": "bc138a94c9644c9da4a3093f20e29890",
            "es_dns": "www.server-cert.com",
            "es_cert_type": 1,
            "es_project_id": "d0599a61793943fba9278165e51e7d52",
            "es_domain_id": "default",
            "es_issuer_ca_id": "65ddc0d1-2793-4bf2-abbb-3eff4e02e26e",
            "es_deleted": false,
            "es_cert_use_type": 1,
            "es_key_algorithm": 1,
            "content_types": {
                "default": "application/octet-stream"
            },
            "secret_ref": "http://barbican-
api.barbican.svc.cluster.local:9311/v1/secrets/5715c3dd-d32c-4edd-9fd1-
5baeb6a8467b"
        }
    ],
    "total": 1
}
```


正常响应代码

200

错误码

400，401，500

注意点

> **独享型负载均衡服务**对接需注意：

- 目前，独享型负载均衡服务创建HTTPS类型的负载均衡监听器时，仅支持 `RSA` 密钥算法类型的服务端证书。因此在创建HTTPS类型的负载均衡监听器获取证书列表时，需要携带以下参数 `show_cert_secrets_only=True&cert_use_type=1&use_es_deleted=True&key_algorithm=1` ；
- 获取证书列表最多只能返回100条数据，如需获取所有证书数据，可通过 `offset` 和 `limit` 参数进行遍历，最后一次遍历返回的数据条数小于 `limit` 参数的值，则证明证书数据已全部取出。

日期	修订内容

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)