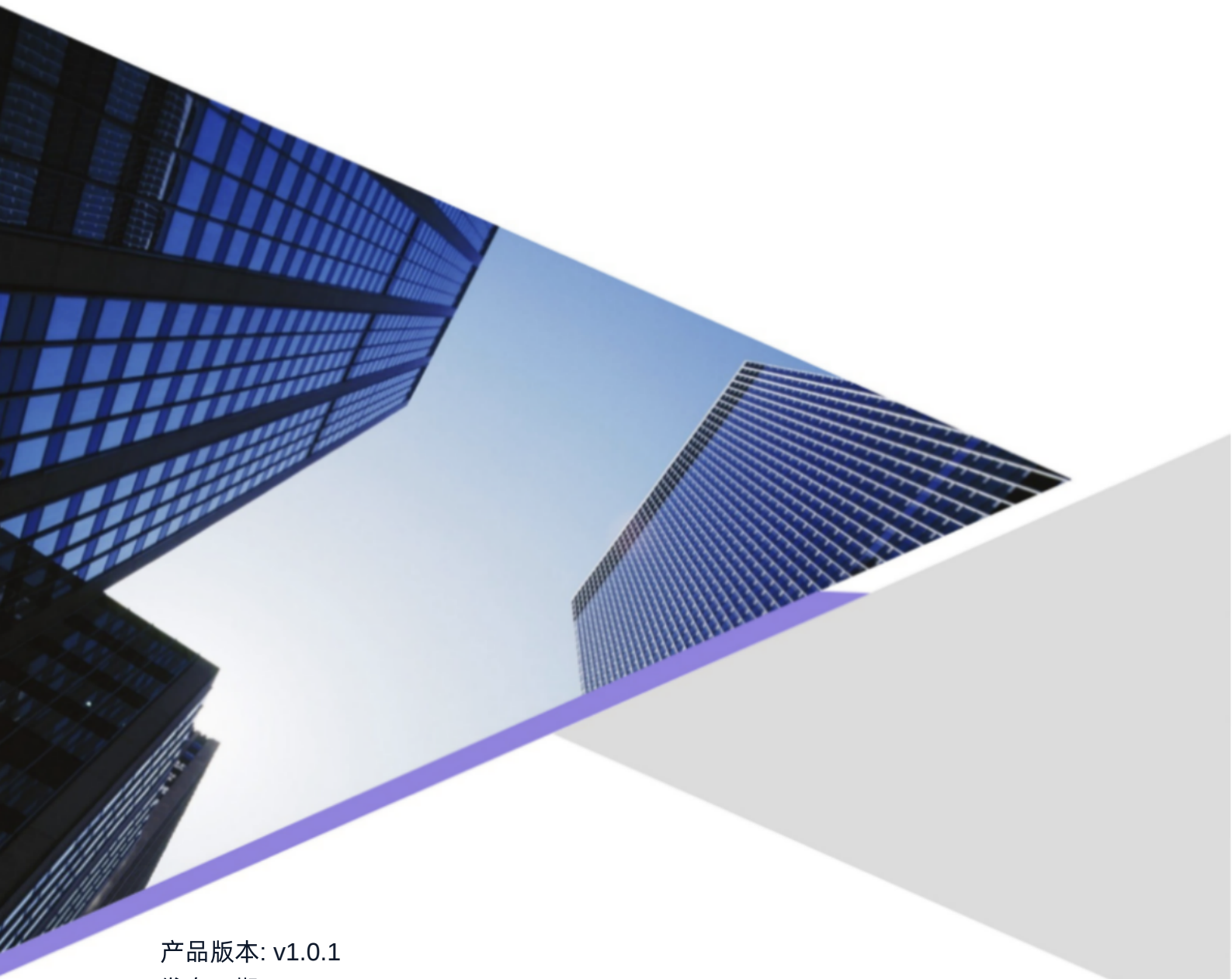
易捷行云
EasyStack

证书服务

产品介绍



产品版本: v1.0.1
发布日期: 2023-06-20

目录

1 产品介绍

1.1 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。

1.2 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。

1.3 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。

1.4 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。

1.5 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。

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)