云证书管理服务

产品介绍

文档版本 08

发布日期 2024-10-11

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

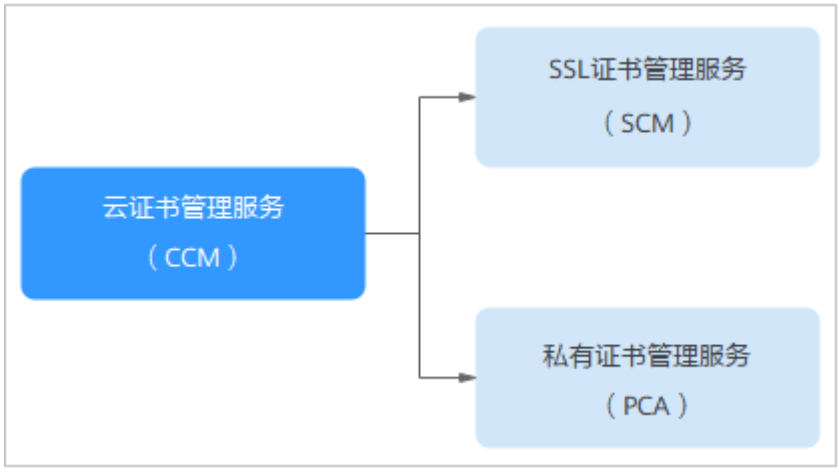
由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 什么是云证书管理服务

云证书管理服务（Cloud Certificate Manager，CCM）是一个为云上海量证书颁发和全生命周期管理的服务。目前，它提供有SSL证书管理（SSL Certificate Manager，SCM）和私有证书管理（Private Certificate Authority，PCA）服务。

图 1-1 云证书管理服务



什么是 SSL 证书管理

SSL证书管理（SSL Certificate Manager，SCM）是一个SSL（Secure Sockets Layer）证书管理平台。它是由华为云联合全球知名数字证书服务机构（CA，Certificate Authority），在华为云平台上为您提供一站式SSL证书的全生命周期管理服务，实现网站的可信认证与安全数据传输。

- 什么是SSL证书?

  SSL证书是一种遵守SSL协议的服务器数字证书，由受信任的根证书颁发机构颁发。

  SSL证书采用SSL协议进行通信，SSL证书部署到服务器后，服务器端的访问将启用HTTPS协议。您的网站将会通过HTTPS加密协议来传输数据，可帮助服务器端和客户端之间建立加密链接，从而保证数据传输的安全。

- 华为云SSL证书管理与HTTPS的关系

  您可以通过华为云SSL证书管理购买SSL证书，并向CA机构提交证书申请，CA机构审核通过后将会签发证书。签发后，您需要将SSL证书下载并安装到Web服务器中

或一键部署至华为云其他云产品中，安装或部署完成后，您的Web服务器或云产品将会通过HTTPS加密协议来传输数据。

- SSL证书的作用
  - 网站身份验证，确保数据发送到正确的客户端和服务器。
  - 在客户端和服务器端之间建立加密通道，保证数据在传输过程中不被窃取或篡改。

什么是私有证书管理

私有证书管理（Private Certificate Authority，PCA）是一个私有CA和私有证书管理平台。您可以通过简单的可视化操作，建立自己完整的CA层次体系并使用它签发证书，实现了在组织内部签发和管理自签名私有证书。主要用于对组织内部的应用身份认证和数据加解密。

私有CA颁发的证书仅在您的组织内受信任，在Internet上不受信任。

2 产品优势

快速签发 SSL 证书

一键申请快捷高效。支持在一个平台下购买签发多个不同品牌的SSL证书。

与知名品牌合作，提供多种 SSL 证书类型

与知名数字证书服务机构合作，确保数字证书认证可信力和加密强度，安全有保障。提供企业型（OV）、企业型专业版（OV Pro）、增强型（EV）、增强型企业版（EV Pro）和基础版（DV）多种证书，便于企业根据自身业务场景灵活选择。

一站 SSL 证书服务

提供一站式云上SSL证书申请、管理、查询、验证等服务，将证书应用到华为云服务的各个环节中。同时，还支持对云下证书进行统一管理，将已签发的第三方SSL证书上传到云证书管理服平台，即可享受查看证书、部署证书、证书到期提醒等功能。

身份认证

身份认证是别的加密方式都不具备的，能在SSL证书信息里面看到网站所有者公司信息，进而确认网站的有效性和真实性，不会被钓鱼网站所欺骗。

一键部署到云产品

支持一键将SSL证书部署在华为云已经开通的云产品中（ELB、CDN、WAF），以最小成本在云上应用。

私有 CA 托管能力

用户无需构建和维护复杂的CA基础设施，在华为云上按需付费即可轻松获得CA管理能力。

完整私有 CA 层次结构

支持创建灵活的CA层次结构，包括根CA和子CA，同时支持外部CA，满足更多应用部署。

私有证书生命周期管理

提供证书、密钥统一管理，具备千万级以上的证书服务管理能力，支持证书撤销列表及时提醒租户证书状态，避免证书过期。

私有证书支持多种密钥算法

支持RSA_2048、RSA_4096、EC_P256、EC_P384等多种密钥算法，支持X.509 v3证书格式，符合PKI/CA国际标准。

私有证书密钥存储安全可靠

通过密钥管理服务（KMS）和硬件安全模块（HSM）提供安全保护，可以安全可靠保存密钥。

私有证书 API 灵活集成

提供丰富的API接口，可以帮助您在开发环境高效集成，快速进行产品部署，为企业租户提供了巨大的灵活性。

3 应用场景

网站可信认证

SSL证书如同网站在互联网中的“身份证”，网站没有安装SSL证书，浏览器将会将其列为不安全的网站，网站用户也就无法信任您网站的安全性，安装了SSL证书就代表您的网站是“安全”的，网站用户可以放心访问您的网站。特别是OV或EV型证书，CA颁发机构在签发证书前会验证域名所有者及其企业信息，可以有效提升网站可信度。

网站数据加密

通常网站数据传输使用的HTTP协议，无法加密数据，导致数据有泄露和被窃听、篡改的风险，SSL证书可以让您的网站采用HTTPS加密通讯，有效提升数据传输安全性。

在华为云 WAF、ELB、CDN 等服务上使用 HTTPS 协议

如果您购买了华为云WAF、ELB、CDN等服务，可以在SSL证书管理页面中将购买的证书一键部署至这些云产品中，为云产品提供HTTPS数据传输安全保障。

提高网站访问速度

SSL 证书全面兼容 HTTP2.0 协议，快速动态加载网页内容，可以为网站服务提速。

企业对内实行应用数据安全管控

您可以通过私有证书管理建立企业内部的证书管理体系，在企业内部签发和管理自签名私有证书，实现企业内部的身份认证、数据加解密、数据安全传输。

车联网应用

车企TSP使用私有证书管理服务，为每台车辆终端颁发证书，提供车-车、车-云、车-路多场景交互时鉴权、认证、加密等安全能力。

物联网应用

IoT平台使用私有证书管理服务，为每台IoT设备颁发证书，并通过IoT平台联动PCA，实现IoT设备的身份校验与认证，保障IoT场景下设备接入安全。

4 产品功能

云证书管理服务提供以下功能，帮助您实现网站HTTPS化，为网站提供安全、有效的访问。

SSL 证书管理

功能名称	功能描述
SSL证书申购	云证书管理服务SSL证书管理提供了OV（企业版）、OV Pro（企业型专业版）、EV（增强型）、EV Pro（增强型专业版）和DV（Basic）基础版五种类型的SSL证书，以及DigiCert、GeoTrust种品牌供您选择。
SSL证书统一管理	云证书管理服务提供上传证书和私钥功能，实现在华为云平台统一管理各种证书、提交审核、查看证书绑定域名和到期时间、修改证书名称、删除已过期的证书等一站式服务，帮助您有效提高证书运维效率。详细操作请参见**上传已有证书**。
SSL证书一键部署	支持一键将数字证书部署在华为云已经开通的云产品中（ELB、CDN、WAF），以最小成本在云上应用。
SSL证书吊销	按照标准的证书吊销流程，经过CA机构审核后，安全、快捷地吊销已签发的SSL证书。
SSL证书退款	SCM支持7天无理由退款，详细操作请参见**退订证书**。
SSL证书续费	SSL证书存在有效期限制。CA机构签发的SSL证书默认有效期为1年，您需要在证书到期前进行续费。详细操作请参见**续费证书**。

私有证书管理

功能名称	功能描述
华为云托管的证书颁发机构	私有证书管理服务提供证书颁发机构（Certificate Authority，CA），支持多种密钥算法，其中包括：RSA_2048、RSA_4096、EC_P256、EC_P384等。支持X.509 v3的证书格式，支持CA多级扩展和多级认证，采用国际通用的对称和非对称算法，符合PKI/CA国际标准。
私有证书生命周期管理	私有证书管理服务提供对私有证书的申请、下载、吊销，具备千万级以上的证书管理能力。
密钥生命周期管理	私有证书管理服务使用华为云的密钥管理服务（Key Management Service，KMS）、硬件安全模块HSM（Hardware Security Module）来保护CA密钥的安全，支持软件和硬件产生密钥对，完成密钥的产生、更新、删除、恢复等功能。
私有证书撤销列表（Certificate Revocation List，CRL）管理	私有证书管理服务能定期自动向您的华为云OBS桶发布和更新证书撤销列表，供您或应用下载。应用程序、服务以及设备可以定期使用CRL评估证书状态。
API自动化集成	私有证书管理服务提供API，可以帮助您在开发环境高效集成，快速进行产品部署。

5 安全

5.1 责任共担

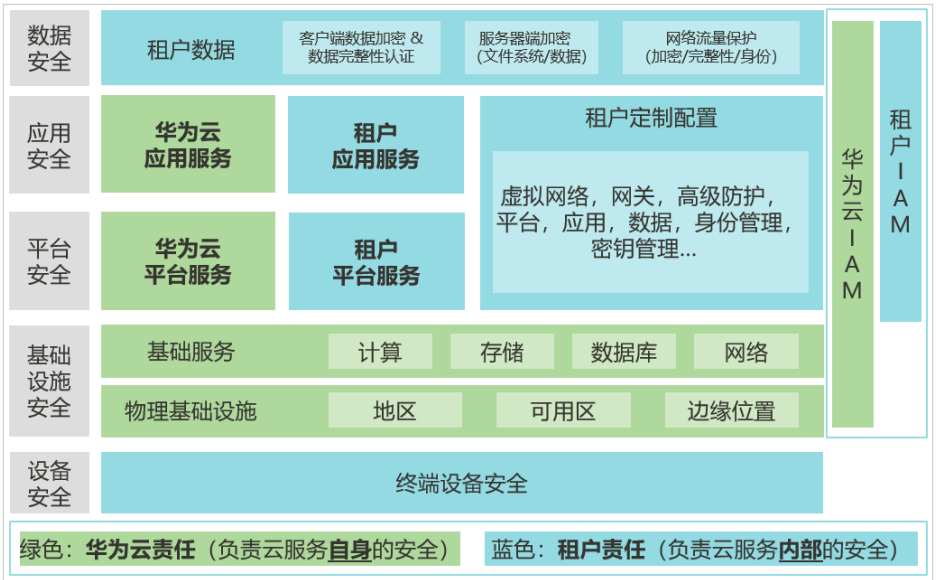
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如图5-1所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的 IaaS、PaaS 和 SaaS 类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。华为云租户的安全责任在于对使用的 IaaS、PaaS 和 SaaS 类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API 网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 5-1 华为云安全责任共担模型



5.2 身份认证与访问控制

CCM对接了统一身份认证服务（Identity and Access Management，IAM）服务。IAM权限是作用于云资源的，IAM权限定义了允许和拒绝的访问操作，以此实现云资源权限访问控制。通过IAM，可以将用户加入到一个用户组中，并用策略来控制他们对华为云资源的访问范围。

关于对CCM资源的访问权限，详细请参考**CCM权限管理**。

5.3 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行**申请下载**合规资质证书。

图 5-2 合规证书下载

资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看**资源中心**。

图 5-3 资源中心

6 CCM 权限管理

如果您需要对华为云上购买的云证书管理服务（CCM）资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在华为云账号中给员工创建IAM用户，并使用策略来控制他们对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有云证书管理服务（CCM）的使用权限，但是不希望他们拥有删除CCM等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用CCM，但是不允许删除CCM的权限策略，控制他们对华为云CCM资源的使用范围。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用CCM服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

CCM 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

CCM部署时不区分物理区域，为全局级服务。授权时，在全局项目中设置权限，访问CCM时，不需要切换区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对CCM服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分，CCM支持的API授权项请参见**权限及授权项说明**。

如表6-1所示，包括了CCM所有系统角色。

表 6-1 CCM 系统角色

角色名称/策略名称	描述	类别	依赖关系
SCM Administrator	SSL证书管理服务管理员权限，拥有服务的所有权限。	系统策略	依赖“Server Administrator”和“Tenant Guest”角色，在同项目中勾选依赖的角色。 购买证书需要依赖 BSS Administrator角色。 BSS Administrator：系统角色，费用中心（BSS）管理员，拥有该服务下的所有权限。 WAF FullAccess：系统策略，Web应用防火墙管理员。 ELB FullAccess：系统策略，弹性负载均衡服务所有权限。 CDN FullAccess：系统策略，具有内容分发网络（CDN）所有细粒度鉴权接口的操作权限。 EPS FullAccess：系统策略，企业项目管理服务所有权限。 OBS Administrator：系统策略 ，对象存储服务管理员。 DNS FullAccess：系统策略，拥有该权限的用户可以拥有云解析服务的全部权限，包括创建、删除、查询、修改等操作。

角色名称/策略名称	描述	类别	依赖关系
SCM FullAccess	SSL证书管理服务的所有权限。	系统策略	购买证书需要依赖 BSS Administrator角色。 BSS Administrator：系统角色，费用中心（BSS）管理员，拥有该服务下的所有权限。 WAF FullAccess：系统策略，Web应用防火墙管理员。 ELB FullAccess：系统策略，弹性负载均衡服务所有权限。 CDN FullAccess：系统策略，具有内容分发网络（CDN）所有细粒度鉴权接口的操作权限。 EPS FullAccess：系统策略，企业项目管理服务所有权限。 OBS Administrator：系统策略 ，对象存储服务管理员。 DNS FullAccess：系统策略，拥有该权限的用户可以拥有云解析服务的全部权限，包括创建、删除、查询、修改等操作。
SCM ReadOnlyAccess	SSL证书管理服务只读权限，拥有该权限的用户仅能查询证书信息，不具备对证书进行增删改权限。	系统策略	无。
PCA FullAccess	私有证书管理服务所有权限。	系统策略	创建私有CA或私有证书需要依赖BSS Administrator角色。 EPS FullAccess：系统策略，企业项目管理服务所有权限。 OBS Administrator：系统策略 ，对象存储服务管理员。

表6-2列出了SSL证书管理常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

须知

如需购买证书，账号除了必须拥有“**SCM Administrator**”或“**SCM FullAccess**”之外，还需要拥有“**BSS Administrator**”权限。

BSS Administrator：费用中心、资源中心、账号中心的所有执行权限。项目级角色，在同项目中勾选。

表 6-2 常用操作与系统权限的关系

操作	SCM Administrator	SCM FullAccess	SCM ReadOnlyAccess
查询SSL证书列表	√	√	√
查询SSL证书详情	√	√	√
查询SSL证书产品类型	√	√	√
查询SSL证书产品详情	√	√	√
取消SSL证书申请	√	√	x
购买SSL证书	√	√	x
申请SSL证书	√	√	x
保存申请SSL证书填写的信息	√	√	x
读取申请SSL证书填写的信息	√	√	√
修改SSL证书	√	√	x
删除SSL证书	√	√	x
下载SSL证书	√	√	x
上传认证信息	√	√	x
吊销SSL证书	√	√	x
推送SSL证书	√	√	x
查询SSL证书推送记录	√	√	√
上传SSL证书	√	√	x
校验CSR	√	√	x
新增附加域名	√	√	x
取消隐私授权	√	√	x
重新签发SSL证书	√	√	x
退订SSL证书	√	√	x

相关链接

- IAM产品介绍
- 创建用户组、用户并授权SCM权限
- 创建用户组、用户并授权PCA权限
- 策略支持的授权项

7 如何选购 SSL 证书

7.1 各类型 SSL 证书之间的区别

华为云SSL证书管理服务提供了DV、OV、EV三种类型的SSL证书。

本章节将介绍各类型证书之间的区别。

说明

特殊企业不支持申请OV、EV类型的证书。例如：军队、政府的一些特殊机构、国家保密单位等。

原因：全国组织机构统一社会信用代码公示查询平台无法在查询到特殊企业的相关信息，因而无法完成组织身份验证，所以特殊企业无法使用OV、EV类型的SSL证书。

证书类型

华为云SSL证书服务支持购买DV、OV和EV三种类型的SSL证书。不同证书类型适用的应用场景、信任等级和安全性不同，具体区别如**表 各种证书之间的区别**所示。

表 7-1 各种证书之间的区别

证书类型	安全等级	认证强度	适用场景	支持的证书品牌	审核时长
DV（域名型）	一般	简易验证域名所有权	个人或企业测试的网站	• DigiCert • GeoTrust	数小时内快速颁发

证书类型	安全等级	认证强度	适用场景	支持的证书品牌	审核时长
OV（企业型）	高	全面验证组织及企业真实性和域名所有权	教育、政府、互联网、中小型企业应用、电商等服务型网站 例如，Apple Store、微信小程序等	• DigiCert • GeoTrust	3～5个工作日
EV（增强型）	最高	严格验证组织及企业真实性和域名所有权	有严格安全要求的大型企业、机构和组织的网站 例如，金融、保险、银行等	• DigiCert	7～10个工作日

证书品牌

目前云证书管理支持购买的证书品牌及不同品牌支持签发的证书类型如下表所示：

表 7-2 证书品牌说明

证书品牌	说明	是否支持DV（域名型）SSL证书	是否支持OV（企业型）SSL证书	是否支持EV（增强型）SSL证书
DigiCert	DigiCert（原Symantec）是全球最大、最权威的数字证书颁发机构。全球著名的数字证书提供商，服务范围超过150多个国家，拥有超过10万客户。 优势：安全、稳定、兼容性好。受银行、金融等行业青睐，适用于高安全性要求的数字交易场景。	是 仅支持单域名。	是 支持单域名、多域名和泛域名。	是 支持单域名、多域名。

证书品牌	说明	是否支持DV（域名型）SSL证书	是否支持OV（企业型）SSL证书	是否支持EV（增强型）SSL证书
GeoTrust	GeoTrust是全球第二大数字证书颁发机构，也是身份认证和信任认证领域的领导者。公司服务于各大中小型企业，一直致力于用最低的价格来为客户提供最好的服务。 优势：该品牌是DigiCert旗下的子品牌。安全、稳定、兼容性好、HTTPS防护门槛低、性价比高。	是 支持单域名、泛域名。	是 支持单域名、泛域名。	是 支持单域名、多域名。

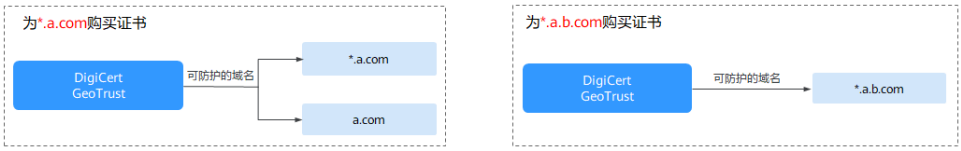
惠赠活动：

- 单域名：以域名www.a.com和根域名a.com为例进行说明

图 7-1 品牌惠赠活动

- 泛域名：以域名*.a.com和*.a.b.com为例进行说明

图 7-2 品牌惠赠活动



证书支持的域名类型

不同域名类型的证书所支持绑定的域名区别如下表所示：

表 7-3 域名类型

域名类型	说明
单域名	即单个SSL证书只支持绑定1个单域名。例如，example.com

域名类型	说明
多域名	即单个SSL证书可以同时绑定多个域名。 • 最多可以支持250个域名。 • 仅当证书类型为OV、OV Pro时，多个域名中可包含泛域名。其他类型的证书，仅支持绑定多个单域名。 • 多个域名可以分批次绑定。例如，购买多域名类型证书，域名数量为3的场景，首次申请证书时仅填写了2个域名，证书签发后可再追加填写1个域名。 • 当购买多域名类型证书，域名数量为3的场景，仅支持绑定3个域名。如果后续还需添加，则需要重新购买证书。
泛域名	即单个SSL证书支持绑定一个且只有一个泛域名。*.*.example.com多个通配符的泛域名不支持。 泛域名只允许添加一个通配符域名，例如*.example.com（包含a.example.com、b.example.com、.....，但是不包含a.a.example.com）。
更多关于如何选择域名类型，详情请参见**如何选择域名类型？**。	

证书支持的加密算法

华为云云证书管理服务签发的SSL证书目前支持RSA、ECC两种加密算法。

- **RSA**：目前在全球应用广泛的非对称加密算法，兼容性在三种算法中最好，支持主流浏览器和全平台操作系统。一般采用2048位或3072位的加密长度。
- **ECC**：椭圆曲线加密算法。相比于RSA，ECC加密速度快、效率更高、服务器资源消耗低，目前已在主流浏览器中得到推广，成为新一代主流算法。一般采用256位加密长度。

不同类型的证书支持的加密算法如**表 证书支持的加密算法**所示。

表 7-4 证书支持的加密算法

证书品牌	证书类型	域名类型	支持的加密算法
DigiCert	DV (Basic)	单域名	RSA_2048、RSA_3072、RSA_4096
	OV	单域名	RSA_2048、RSA_3072、RSA_4096、EC_P256、EC_P384
		多域名	RSA_2048、RSA_3072、RSA_4096、EC_P256、EC_P384
		泛域名	RSA_2048、RSA_3072、RSA_4096、EC_P256、EC_P384
	OV Pro	单域名	RSA_2048、RSA_3072、RSA_4096、EC_P256、EC_P384

证书品牌	证书类型	域名类型	支持的加密算法
		多域名	RSA_2048、RSA_3072、RSA_4096、EC_P256、EC_P384
		泛域名	RSA_2048、RSA_3072、RSA_4096、EC_P256、EC_P384
	EV	单域名	RSA_2048、RSA_3072、RSA_4096、EC_P256、EC_P384
		多域名	RSA_2048、RSA_3072、RSA_4096、EC_P256、EC_P384
	EV Pro	单域名	RSA_2048、RSA_3072、RSA_4096、EC_P256、EC_P384
		多域名	RSA_2048、RSA_3072、RSA_4096、EC_P256、EC_P384
GeoTrust	DV (Basic)	单域名	RSA_2048、RSA_3072、RSA_4096
		泛域名	RSA_2048、RSA_3072、RSA_4096
	OV	单域名	RSA_2048、RSA_3072、RSA_4096、EC_P256、EC_P384
		泛域名	RSA_2048、RSA_3072、RSA_4096、EC_P256、EC_P384

7.2 证书选型案例

表 7-5 以下为部分典型行业证书选型案例，您在选购证书时可以进行参考。

实例	所属行业	业务特征	常用证书类型
• 中国农业银行 • 中国平安	金融、银行、保险	• 有严格的数据保密要求 • 希望在网站地址栏展示身份信息	EV

实例	所属行业	业务特征	常用证书类型
• 教育部 • 淘宝、京东 • 百度、新浪、今日头条 • 上海证券交易所 • 国家电网 • 外交部 • 华为云	教育、政府、互联网	• 有严格的数据保密要求 • 无需在网站地址栏展示身份信息 • 网站后期有多个新增站点的需求	OV泛域名证书
个人网站	个人业务	• 无数据传输业务 • 网站用来展示纯信息或内容	DV

8 基本概念

8.1 SCM 相关概念

本章节介绍与华为云SCM服务相关的概念及其解释。

数字证书

数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。它是权威机构颁发给网站的可信凭证。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。数字证书还有一个重要的特征就是只在特定的时间段内有效。

SSL 协议

SSL协议又称为“安全套接层”（Secure Sockets Layer）协议，是通过计算机网络提供通信安全性的加密协议。可在浏览器和网站之间建立加密通道，保证信息传输过程中不被窃取、篡改。

CA 机构

CA机构，又称CA认证中心，即证书授权中心（Certificate Authority），或称证书授权机构，是负责发放和管理数字证书的权威机构，并作为电子商务交易中受信任的第三方，承担公钥体系中公钥合法性检验的责任。

HTTPS

HTTPS是一种基于SSL协议的网站加密传输协议。网站安装SSL证书后，使用HTTPS加密协议访问，可以激活客户端浏览器到网站服务器之间的“SSL加密通道”（SSL协议），实现高强度双向加密传输，防止传输数据被泄露或篡改。简单讲就是HTTP的安全版。

CSR

CSR（Cerificate Signing Request）即证书签名请求文件，是申请证书时申请者发给证书颁发机构（CA）用于申请SSL证书的。CSR包含了公钥和标识名称（Distinguished Name），通常从Web服务器生成CSR，同时创建加解密的公钥私钥对。

SSL 证书有效期

自2020年9月1日起，全球CA机构颁发的SSL证书有效期最长为一年。因此，您通过华为云云证书服务申请的SSL证书，有效期都是一年。

8.2 PCA 相关概念

本章节介绍与华为云PCA服务相关的概念及其解释。

根 CA

颁发机构（CA）的公钥证书，是公钥基础设施（PKI）体系中的信任锚。可签发子CA、私有证书与证书吊销列表。当被导入客户端信任列表后，可对其签发的证书进行校验。

子 CA

也称中间CA或子CA，用于隔绝根CA与私有证书，是划分CA层次结构的关键，在证书链校验过程中对下一层证书进行校验。当路径深度大于0时，子CA可向下签发子CA。

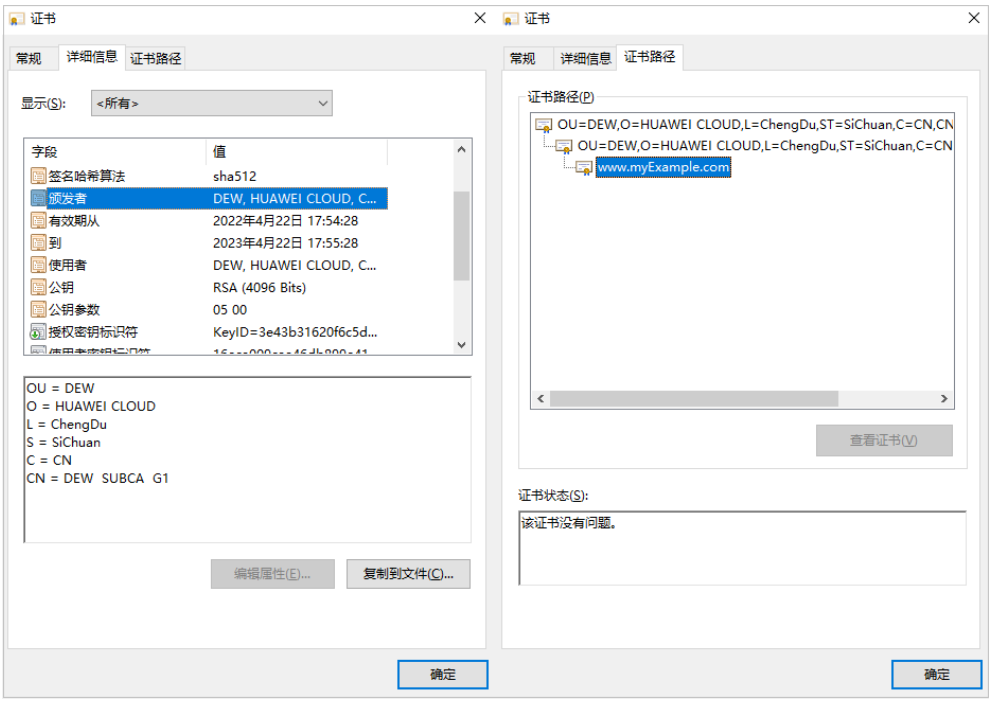
说明

子CA的路径深度，即当前CA可以签发下级子CA的层次数量，用于控制证书链深度（证书链最后一层为私有证书）。

私有证书

私有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。私有证书内容，如图 私有证书所示。

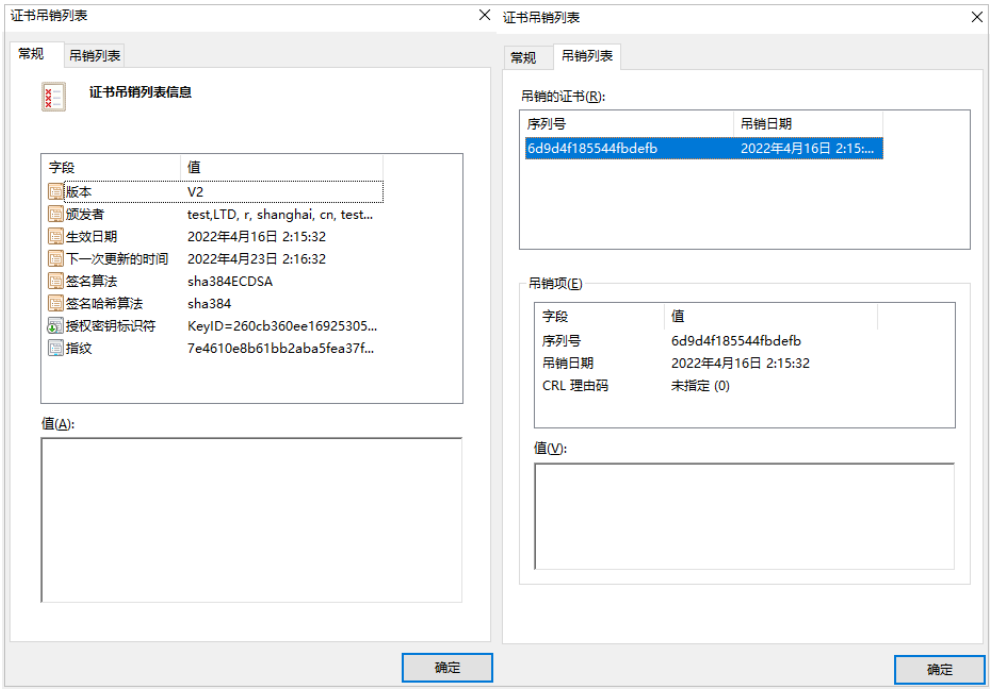
图 8-1 私有证书



证书吊销列表

证书吊销列表（Certificate Revocation List，CRL）是指在有效期内就被其父CA吊销的证书的名单，其中被吊销的证书类型，包含子CA与私有证书。证书吊销列表是一种有固定格式的结构化数据文件，其中包含颁发者信息、吊销列表的生效时间、列表下一次更新时间、签发算法、指纹以及已被吊销证书的序列号与对应的吊销时间和吊销理由码。证书吊销列表具体内容，如**图 证书吊销列表**所示。

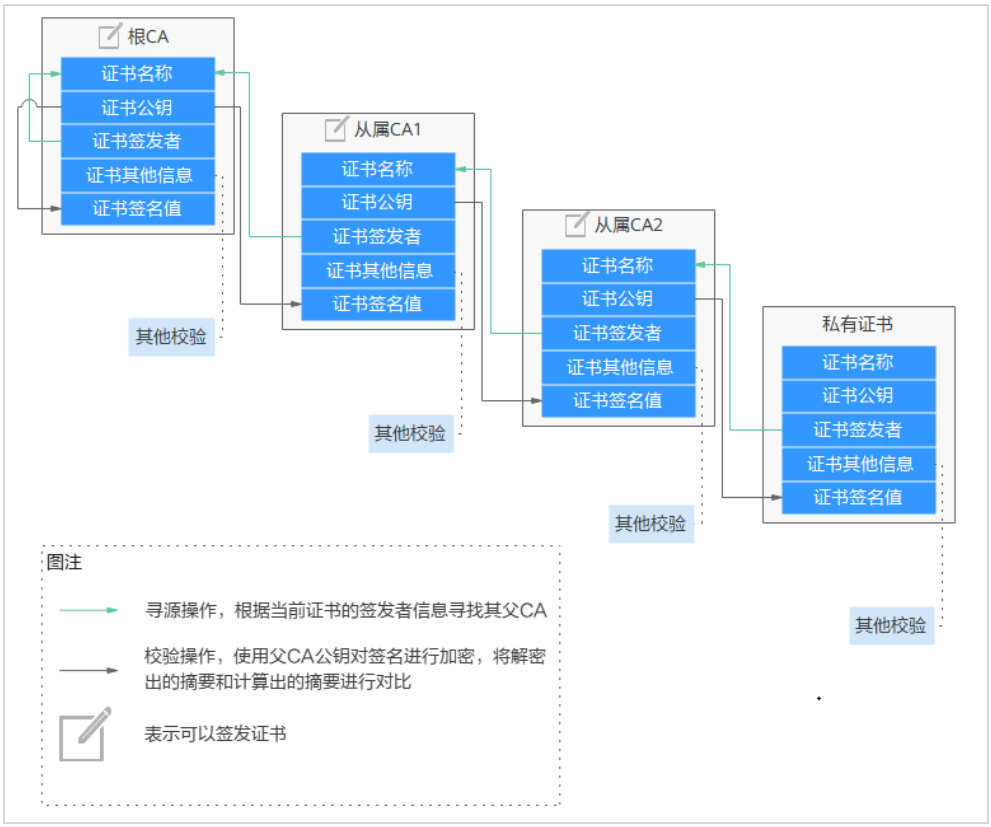
图 8-2 证书吊销列表



证书链

从根CA到私有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。各级证书的链接关系，如**图 证书链**所示。

图 8-3 证书链



证书校验主要体现在两方面：

- 证书链的完整性校验，逐层校验证书的有效性。
- 证书链中的根CA是否被校验方所信任（提前预置到信任列表中）。

证书校验过程中主要包含的校验项：

- 实体所宣称的主体信息（如服务端的域名）是否在证书可选名称的范围内。
- 证书是否过期。
- 密钥用法是否符合当前操作（如密钥协商、数字签名等）。
- 数字签名验证。
- 是否已被吊销。

说明

此处未列举出所有校验项，X509证书允许用户增加多种自定义扩展项，详情请参考相关国际标准。

PCA 证书有效期

在证书链中，根CA是整条链的信任起点，一旦根CA过期，其与其子CA签发的所有证书将不再被信任，因此根CA的有效期是其下层所有证书的有效期上限。即使签发下层证书时，可以将有效期填写超过根CA的有效期（不做强制要求下），但在校验证书链时，只要链中根CA过期，校验就会失败。

在PCA服务中，强制要求新签发的证书的到期时间不可超过其父CA的到期时间，确保从根CA到私有证书之间的链路上，有效期逐层递减。PCA服务对各类证书有效期的约束见**表 证书有效期约束**。

不同类型证书的有效期是根据其扮演的角色而定的。使用越频繁的证书，其密钥材料泄露风险更高，有效期应尽量设置更小。例如，根CA通常只用于签发子CA，使用频率最少，且使用最高的安全保护措施（PCA中使用KMS进行CA密钥管理），有效期一般设置为10~30年左右。子CA根据其所在的层级，越往下有效期逐级减少，最下层的证书用于签发大量的私有证书，有效期通常设置为2~5年左右。私有证书，频繁用于通信，通常根据使用场景的安全要求，将有效期设置为几个小时、几个月以及一两年不等。

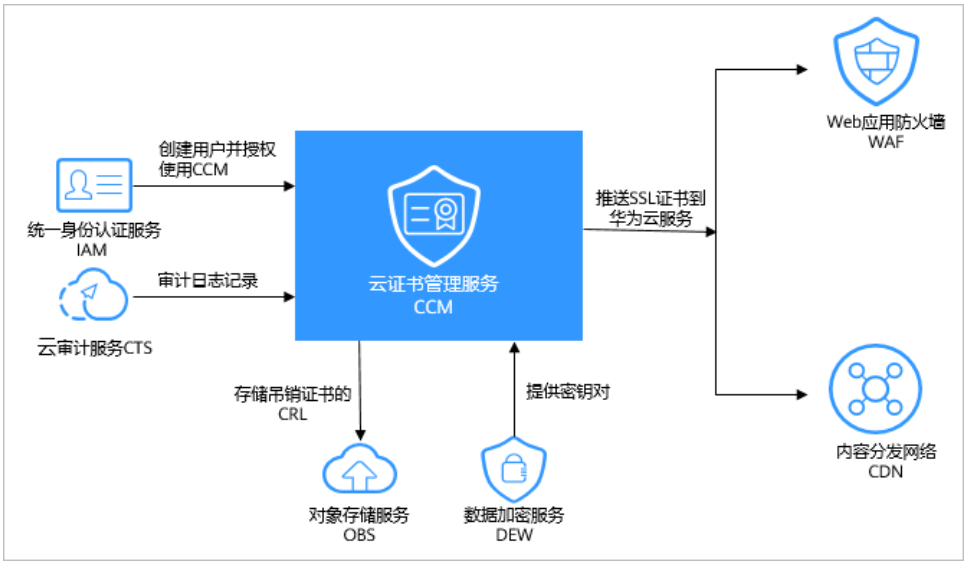
表 8-1 证书有效期约束

证书类型	最小有效期	最大有效期	是否支持延长	有效期其它约束
根CA	1小时	30年	否	无
子CA	1小时	20年	否	在父CA有效期内
私有证书	1小时	20年	否	在父CA有效期内

9 与其他云服务的关系

云证书管理服务与周边服务的依赖关系如图9-1所示。

图 9-1 与其他云服务的关系



与 Web 应用防火墙的关系

用户可以在SSL证书管理平台购买SSL证书，再将其一键部署到Web应用防火墙（Web Application Firewall，简称WAF）中。

与 CDN 的关系

用户可以在SSL证书管理平台购买SSL证书，再将其一键部署到CDN（Content Delivery Network，内容分发网络）中。

与对象存储服务的关系

对象存储服务（Object Storage Service，简称OBS）是一个基于对象的海量存储服务，为客户提供海量、安全、高可靠、低成本的数据存储能力。私有证书管理服务中执行吊销证书操作时，吊销证书的CRL会存储在用户的OBS桶里，供客户查询。

与数据加密服务的关系

数据加密服务（Data Encryption Workshop，DEW）为云证书管理服务提供密钥对生成及保护的功能。详细内容请参考**数据加密服务用户指南**。

与云审计服务的关系

云审计服务（Cloud Trace Service，CTS）记录云证书管理服务的相关的操作事件，方便用户日后的查询、审计和回溯。详细内容请参考**云审计服务用户指南**。

与统一身份认证服务的关系

统一身份认证服务（Identity and Access Management，简称IAM）为云证书管理服务提供了权限管理的功能。

需要拥有PCA FullAccess和SCM FullAccess权限的用户才能使用CCM。

如需开通该权限，请联系拥有Security Administrator权限的用户。详细内容请参考**统一身份认证服务用户指南**。

10 个人数据保护机制

为了确保您的个人数据（例如用户名、密码、手机号码等）不被未经过认证、授权的实体或者个人获取，CCM通过加密存储个人数据、控制个人数据访问权限以及记录操作日志等方法防止个人数据泄露，保证您的个人数据安全。

收集范围

CCM收集及产生的个人数据如表10-1所示：

表 10-1 个人数据范围列表

类型	收集方式	是否可以修改	是否必须
租户ID	• 在控制台进行任何操作时Token中的租户ID • 在调用API接口时Token中的租户ID	否	是，租户ID是证书资源身份标识
姓名	在申请SSL证书时填写的联系人姓名	是	是，证书审核人工认证阶段必须
邮箱	在申请SSL证书或私有证书时填写的邮箱	• 申请SSL证书时填写的邮箱：是 • 申请私有证书时填写的邮箱：否	• 申请SSL证书时填写的邮箱：是，证书审核人工认证阶段必须 • 申请私有证书时填写的邮箱：否
手机号码	在申请SSL证书时填写的联系人手机号	是	是，证书审核人工认证阶段必须
企业营业执照	在申请SSL证书时，可以选择上传企业营业执照	是	否
银行开户许可	在申请SSL证书时，可以选择上传银行开户许可	是	否

类型	收集方式	是否可以修改	是否必须
企业项目ID	在申请或使用SSL证书、私有证书时，可以为证书分配企业项目	是	已开通企业项目：是 未开通企业项目：否

存储方式

CCM通过加密算法对您个人敏感数据加密后进行存储。

- 租户ID：不属于敏感数据，明文存储
- 姓名、邮箱、手机号码：加密存储

访问权限控制

您的个人数据通过加密后存储在CCM数据库中，访问个人数据需要通过Token认证。

日志记录

您的个人数据的所有操作，包括修改、查询和删除等，CCM都会记录审计日志并上传至云审计服务（CTS），您可以并且仅可以查看自己的审计日志。