SSL 证书管理

产品介绍

文档版本 22

发布日期 2021-01-26

华为技术有限公司

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，华为公司对本文档内容不做任何明示或默示的声明或保证。

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 SSL 证书管理..... 1
2 各证书之间的区别..... 2
3 功能特性..... 7
4 应用场景..... 9
5 产品优势..... 10
6 计费说明..... 12
7 SCM 权限管理..... 13
8 与其他云服务的关系..... 16
9 个人数据保护机制..... 18
10 相关概念..... 20
A 修订记录..... 21

1 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，平台联合全球知名数字证书服务机构为用户提供购买SSL证书的功能，用户也可以将本地的外部SSL证书上传到平台，实现用户对内部和外部SSL证书的统一管理。

SSL 证书的作用

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。

其主要作用如下：

- 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。

另外，SSL协议，全称为：安全套接层协议(Secure Sockets Layer)，它指定了在应用程序协议（如HTTP、Telnet、FTP）和TCP/IP之间提供数据安全性分层的机制，它是在传输通信协议（TCP/IP）上实现的一种安全协议，采用公开密钥技术，它为TCP/IP连接提供数据加密、服务器认证、消息完整性以及可选的客户机认证。由于SSL协议很好地解决了互联网明文传输的不安全问题，很快得到了业界的支持，并已经成为国际标准。

数字证书的原理

数字证书采用公钥体制，即利用一对互相匹配的密钥对进行加密、解密。每个用户自己设定一把特定的仅为本人所知的私有密钥（私钥），用它进行解密和签名；同时设定一把公共密钥（公钥）并由本人公开，为一组用户所共享，用于加密和验证签名。

由于密钥仅为本人所有，这样就产生了别人无法生成的文件，也就形成了数字签名。

数字证书是一个经证书授权中心（CA）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。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。

2 各证书之间的区别

目前，华为云SSL证书管理服务提供了OV（企业版）、OV Pro（企业型专业版）、EV（增强型）、EV Pro（增强型专业版）、DV（域名型）和DV（Basic）基础版六种类型的SSL证书，以及DigiCert、GlobalSign、GeoTrust三种品牌供您选择。同时，SSL证书管理提供了CFCA国密证书供您使用。

说明

- CFCA国密证书暂不支持控制台购买，如果您需要使用此证书，需要在管理控制台的右上角，单击“工单 > 新建工单”，通过工单申请。
- 因为无法在全国组织机构统一社会信用代码公示查询平台查询到特殊企业（军队、政府的一些特殊机构、国家保密单位等）的相关信息，导致无法完成组织身份验证，所以特殊企业无法使用企业型（OV、OV Pro）SSL证书以及增强型（EV、EV Pro）SSL证书。

证书品牌

SSL证书支持的品牌包括“DigiCert”、“GlobalSign”、“GeoTrust”，各证书品牌的说明如表2-1所示。

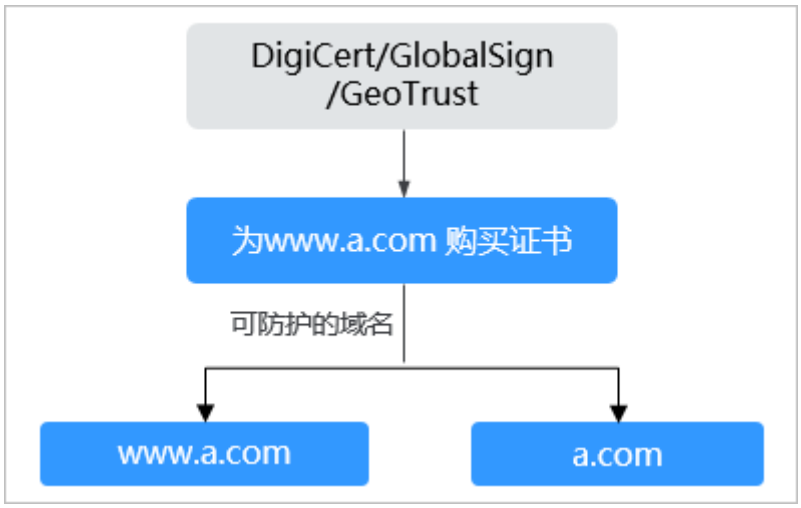
表 2-1 证书品牌说明

证书品牌	证书说明
DigiCert	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。
GlobalSign	一家声誉卓著，备受信赖的CA中心和SSL数字证书提供商，并在全球拥有众多合作伙伴。
GeoTrust	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。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。

各个证书品牌针对www型域名有如下惠赠活动（以域名www.a.com和根域名a.com为例进行说明）：

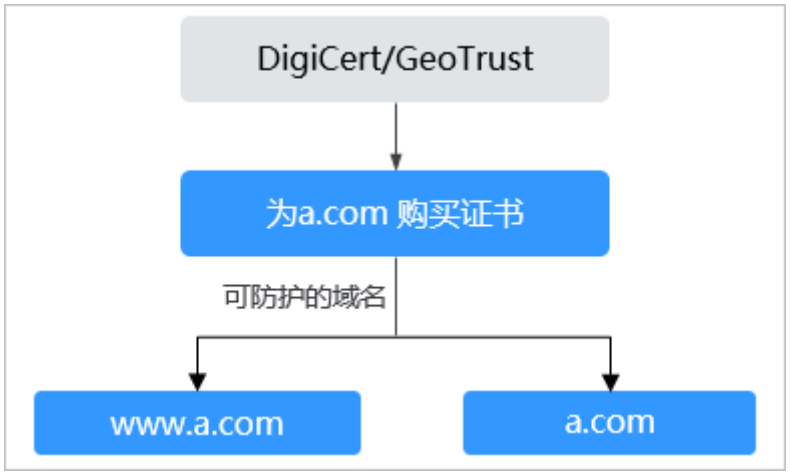
- DigiCert、GlobalSign和GeoTrust三个品牌，为www.a.com购买的证书，该证书同时支持防护a.com域名，如图2-1所示。

图 2-1 为 www.a.com 购买证书



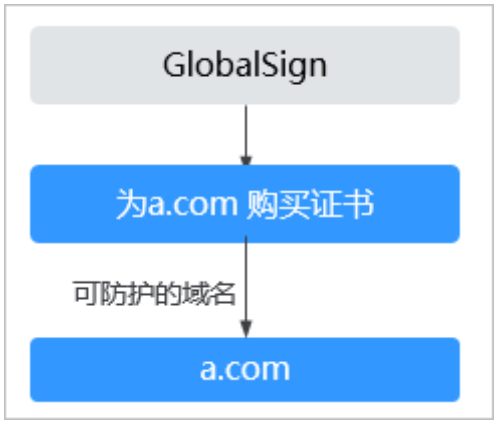
- DigiCert和GeoTrust两个品牌，为a.com购买的证书，该证书同时支持防护www.a.com域名，如图2-2所示。

图 2-2 为 a.com 购买证书



- GlobalSign品牌，为a.com购买的证书，该证书只支持防护a.com这个域名，不支持防护www.a.com域名，如图2-3所示。

图 2-3 GlobalSign 品牌



证书品牌及支持的域名类型

各个类型的证书支持选择的证书品牌，以及可以保护的域名类型如表2-2。

表 2-2 各种证书之间的区别（一）

证书类型	证书品牌	保护域名的类型	说明
EV Pro ：增强型专业版（Extended Validation Pro）SSL证书	DigiCert	• 单域名 • 多域名	• 对申请者做严格的身份审核验证，信任等级高。 • 加密性能好（采用ECC椭圆曲线算法）。 • 支持最多绑定100个域名；由于EV Pro型证书对域名审核更严格，因此EV Pro型证书暂时没有泛域名的类型。
EV：增强型（Extended Validation）SSL证书	DigiCert、GlobalSign、GeoTrust	• 单域名 • 多域名	• 对申请者做严格的身份审核验证，信任等级高。 • 提供高强度通信链路加密功能，保护内外部网络上敏感数据传输。 • 支持最多绑定100个域名；由于EV型证书对域名审核更严格，因此EV型证书暂时没有泛域名的类型。
OV Pro：企业型专业版（Organization Validation Pro）SSL证书	DigiCert	• 单域名 • 多域名 • 泛域名	• 对申请公司单位做严格的身份审核验证。 • 安全加密算法强度更高（采用ECC椭圆曲线算法） • 支持最多绑定100个域名；支持绑定通配符域名。
OV：企业型（Organization Validation）SSL证书	DigiCert、GlobalSign、GeoTrust **说明** GlobalSign品牌提供该类型的单域名的纯IP证书。	• 单域名 • 多域名 • 泛域名	• 对申请公司单位做严格的身份审核验证。 • 提供高强度通信链路加密功能，保护内外部网络上敏感数据传输。 • 支持最多绑定100个域名；支持绑定通配符域名。
DV：域名型（Domain Validation）SSL证书	GeoTrust	单域名	• 只对网站域名进行简易验证，数小时内即可颁发。 • 提供高强度通信链路加密功能，能起到加密传输的作用，但无法向用户证明网站的真实身份。 • 仅支持绑定一个单一域名。

证书类型	证书品牌	保护域名的类型	说明
DV（Basic）：基础版（Domain Validation）SSL证书	DigiCert、GeoTrust **说明** DigiCert品牌提供该类型的单域名免费证书。	• 单域名 • 泛域名	• 只对网站域名进行简易验证，数小时内即可颁发。 • 只提供通信链路加密功能，能起到加密传输的作用，但无法向用户证明网站的真实身份。 • GeoTrust入门级SSL证书支持选择单域名和泛域名类型的证书。 • DigiCert免费SSL证书仅支持绑定一个单一域名。

应用场景

不同证书类型适用的应用场景、信任等级、认证强度和安全性如表2-3所示。

表 2-3 各种证书之间的区别（二）

证书类型	典型应用场景	信任等级	认证强度	安全性
EV Pro	金融、保险、银行等有更高安全要求的机构和组织。	最高	严格认证	最高（地址栏绿色）
EV	有严格安全要求的大型企业。	最高	严格认证	最高（地址栏绿色）
OV Pro	对数据安全有较高要求的中小型企业应用、电商等服务，支持各类应用，如Apple Store、微信小程序等。	高	CA机构审核组织及企业真实性	高
OV	中小型企业应用、电商等服务，支持各类应用，如Apple Store、微信小程序等。 **说明** GlobalSign品牌提供该类型的单域名的纯IP证书。	高	CA机构审核组织及企业真实性	高
DV	个人网站、企业测试。	一般	CA机构审核个人网站真实性、不验证企业真实性	一般

证书类型	典型应用场景	信任等级	认证强度	安全性
DV（Basic）	非商业场景（如个人、企业测试等）。 **说明** DigiCert品牌提供该类型的单域名免费证书。	一般	CA机构审核个人网站真实性、不验证企业真实性	一般

安全锁和 Https 标志

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。同时，浏览器也会有安全锁的标志。

不同类型SSL证书在加密算法、部署后浏览器显示等方面的区别如表2-4所示。

表 2-4 各种证书之间的区别（三）

证书类型	安全锁	Https标志	显示企业名称	算法支持
EV Pro	√	√	√	仅DigiCert品牌支持该类型证书，支持的算法为RSA+ECC。
EV	√	√	√	不同品牌支持的算法有所不同： • DigiCert：RSA • GlobalSign：RSA+ECC • GeoTrust：RSA
OV Pro	√	√	-	仅DigiCert品牌支持该类型证书，支持的算法为RSA+ECC。
OV	√	√	-	不同品牌支持的算法有所不同： • DigiCert：RSA • GlobalSign：RSA+ECC • GeoTrust：RSA
DV	√	√	-	仅GeoTrust品牌支持该类型证书，支持的算法为RSA。
DV（Basic）	√	√	-	GeoTrust和DigiCert品牌支持该类型证书，支持的算法为RSA。

3 功能特性

华为云SSL证书管理提供以下功能，帮助您实现网站的HTTPS化，为网站提供安全、有效的访问。

购买证书

用户可以购买SSL证书。

SSL证书管理支持申请绑定域名的证书，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）、DV（域名型）和DV（Basic）基础版六种类型的SSL证书，以及DigiCert、GlobalSign、GeoTrust三种品牌供您选择。

同时，还支持申请绑定纯IP的证书，详细操作请参见**申请纯IP证书**。

上传证书

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。具体的参见**上传已有证书**。

吊销证书

证书便捷吊销。按照标准的证书吊销流程，经过CA认证中心审核后，安全、快捷地吊销服务器SSL证书。具体请参见**吊销证书**。

撤回证书申请

证书未签发前，即证书状态为“待完成域名验证”、“待完成组织验证”或“CA审核中（追加域名）”，如果发现证书信息填写错误，此时，可撤回证书申请，重新申请证书。具体的操作请参见**撤回证书申请**。

当用户已提交审核，域名注册平台DNS或者用户信息正在审核中，此时用户可以撤回申请。

重新签发

如果您的证书在已签发后，需要重新绑定域名，可以通过SCM平台的重新签发功能，取消已签发证书，绑定新的域名，重新签发新的证书。

证书签发后，各证书品牌针对证书重新签发的时间有以下限制：

- GlobalSign品牌：5天。
- DigiCert品牌和GeoTrust品牌：25天。

在规定时间内，证书可重新签发的次数不限，超过各证书品牌的规定的时间，将不能执行重新签发的操作。

推送证书

用户可以在SSL证书管理平台上一键推送证书到华为云其他云产品中，帮助您实现低成本部署数字证书。具体请参见**推送证书到云产品**。

管理证书

用户可以修改证书名称、编辑证书描述信息、下载和删除证书。

4 应用场景

用户可以通过SCM获取SSL证书，将证书部署到网站、企业应用或其他服务。

部署后，可以将服务使用的HTTP协议替换成HTTPS协议，帮助用户避免HTTP协议的如下隐患：

- HTTP协议在客户端与服务器端之间使用明文传输数据，可以被轻松截取或篡改。
- HTTP协议不能鉴别真实与虚假网站，因此容易被欺诈、钓鱼网站利用从而导致用户信息泄露、财产损失。

具体应用在以下几方面：

- 网站可信认证：

  适用于网站建设。为用户建立的网站提供基于数字证书的可信身份认证支持，避免网站被仿冒。
- 应用可信认证：

  适用于云应用服务、移动应用服务。为用户云上的应用（CRM、OA、ERP等）提供基于数字证书的可信身份认证支持，避免接入非法应用。
- 应用数据传输保护：

  适用于网站、应用与客户端之间的数据传输。对客户端与网站、应用之间的传输数据加密，防止数据中途被窃取，维护数据完整性，防止被篡改。

5 产品优势

华为云SSL证书有以下几点优势：

安全可靠

基于华为一流的高安全密码解决方案实现证书及相关信息的安全管理，并提供分布式存储与服务架构确保证书服务的高可靠性。

一站服务

提供一站式云上证书申请、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。

自主选择

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）、域名型（DV）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。

专业快速

专业的运营人员全天在线，随时解答您在证书使用的任何疑问。信息、资料齐全者最快可24小时内完成证书签发。

简单快捷

只需要申请一张证书，将证书部署在服务器上就可以在有效期内不用再做其他的操作。

显示直观

部署SSL证书后，通过https访问网站时，在地址栏或地址栏右侧有加密锁标志，能直观的表明网站是加密的。使用EV证书，公司名称能直接显示在地址栏。

身份认证

身份认证是别的加密方式都不具备的，能在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。

快速签发

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数字证书。

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。

6 计费说明

计费项

华为云SSL证书管理服务根据您选择的证书类型、证书品牌、域名类型、域名数量和购买时长进行收费。

计费模式

SSL证书属于按需计费，且为一次性计费产品。

详细的服务资费费率标准，请参见**产品价格详情**。

变更配置

SSL证书购买后，将无法修改证书品牌、证书类型、域名类型、域名数量、有效期、购买量。

如需变更，请重新购买。

续费

证书签发后，到期时间立刻生成且不可修改和延长。证书到期后无法续费，只能重新购买并申请新证书。

到期与欠费

证书到期后，将无法继续使用。您需要在您的证书到期前重新购买。

SSL证书管理控制台会在证书到期前30天提醒您证书即将到期。已签发的证书，SSL证书管理系统还会在证书到期前两个月、一个月、一周和到期时，发送邮件和短信提醒用户。

相关问题

- **SSL证书过期了怎么办?**
- **SSL证书即将到期，该如何处理?**
- **证书是否支持续费?**
- **SSL证书到期后不续费，会影响业务吗?**

7 SCM 权限管理

如果您需要对华为云上购买的SCM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，您可以在华为云帐号中给员工创建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SCM的使用权限，但是不希望他们拥有删除SCM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SCM，但是不允许删除SCM的权限策略，控制他们对SCM资源的使用范围。

如果华为云帐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SCM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，您只需要为您帐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》**。

SCM 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。

SCM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SCM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SCM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，SCM支持的API授权项请参见**权限及授权项说明**。

如**表7-1**所示，包括了SCM的所有系统权限。

表 7-1 SCM 系统权限

系统角色/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。	系统角色	依赖“Server Administrator”和“Tenant Guest”角色，在同项目中勾选依赖的角色。
SCM FullAccess	SSL证书管理服务的所有权限。	系统策略	无。
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。

表7-2列出了SCM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。

表 7-2 常用操作与系统权限的关系

操作	SCM Administrator	SCM FullAccess	SCM ReadOnlyAccess
查询证书列表	√	√	√
查询证书详情	√	√	√
查询证书产品类型	√	√	√
查询证书产品详情	√	√	√
取消申请	√	√	x
购买证书	√	√	x
申请证书	√	√	x
保存申请证书填写的信息	√	√	x
读取申请证书填写的信息	√	√	√
修改证书	√	√	x
删除证书	√	√	x
下载证书	√	√	x
上传认证信息	√	√	x

操作	SCM Administrator	SCM FullAccess	SCM ReadOnlyAccess
吊销证书	√	√	x
推送证书	√	√	x
查询推送记录	√	√	√
上传证书	√	√	x
校验CSR	√	√	x
新增附加域名	√	√	x
取消隐私授权	√	√	x

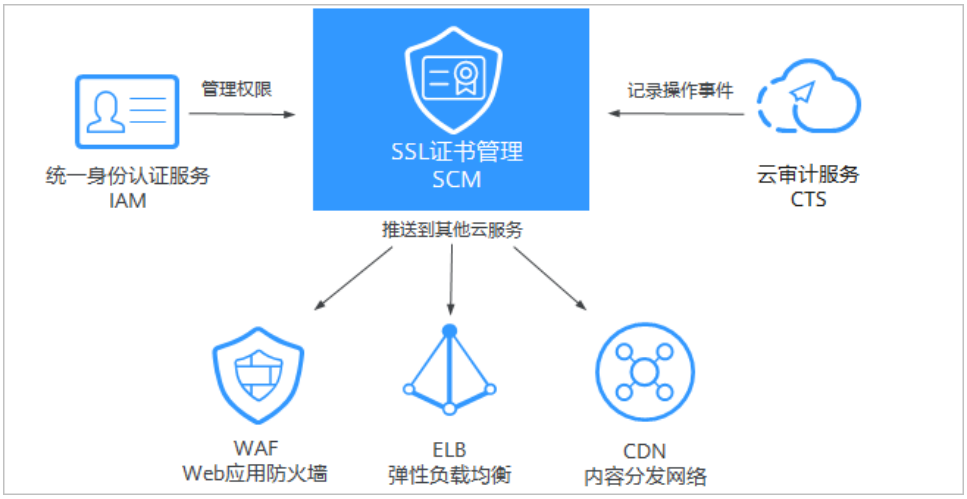
相关链接

- IAM产品介绍
- 创建用户组、用户并授予SCM权限
- 权限及授权项说明

8 与其他云服务的关系

本章节介绍SSL证书管理与其他云服务的关系如图8-1所示。

图 8-1 SSL 证书管理与其他云服务的关系示意图



与弹性负载均衡的关系

用户可以在SSL证书管理平台购买SSL证书，再将其部署到弹性负载均衡（Elastic Load Balance，简称ELB）中。

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，再将其部署到CDN（Content Delivery Network，内容分发网络）中。

与云审计服务的关系

云审计服务（Cloud Trace Service，CTS）记录SSL证书管理平台的相关的操作事件，方便用户日后的查询、审计和回溯，具体请参见《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SSL证书管理提供了权限管理的功能。

需要拥有“SCM Administrator”权限的用户才能使用SCM。

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》。

9 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，SCM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

SCM收集及产生的个人数据如表9-1所示：

表 9-1 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
联系人姓名	在申请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
联系人邮箱	在申请证书时填写的联系人邮箱	是	是，证书审核人工认证阶段必须
联系人手机号码	在申请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	在申请证书时，可以选择上传银行开户许可	是	否

存储方式

SCM通过加密算法对用户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
- 联系人姓名、联系人邮箱、联系人手机号码、企业营业执照、银行开户许可：加密存储

访问权限控制

用户个人数据通过加密后存储在SCM数据库中，访问个人数据需要通过Token认证。

日志记录

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

10 相关概念

本章节介绍与华为云SSL证书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 认证中心

CA认证中心，又称CA机构，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。

A 修订记录

发布日期	修改说明
2021-01-26	第二十二次正式发布。 新增重新签发功能相关描述。
2021-01-20	第二十一次正式发布。 华为云“帐号”词条变更。
2020-12-15	第二十次正式发布。 修改**证书品牌及支持的域名类型**。
2020-11-26	第十九次正式发布。 修改**证书品牌**，增加证书品牌的惠赠活动。
2020-11-17	第十八次正式发布。 修改**证书品牌**，增加了证书区别的描述。
2020-11-03	第十七次正式发布。 修改**各证书之间的区别**，修改了Section标题。
2020-10-29	第十六次正式发布。 • 增加**各证书之间的区别**章节。 • 优化**功能特性**章节。 • 优化**产品优势**章节。
2020-08-26	第十五次正式发布。 修改**SSL证书管理**章节，增加了CFCA国密证书的说明。
2020-08-20	第十四次正式发布。 修改**计费说明**章节。
2020-05-26	第十三次正式发布。 新增DV基础版证书的购买，以及刷新相关内容描述。

发布日期	修改说明
2020-05-20	第十二次正式发布。 • 新增免费证书的购买，以及刷新相关内容描述。 • 新增**计费说明**章节。
2020-04-28	第十一次正式发布。 Symantec品牌SSL证书更名DigiCert品牌SSL证书。
2020-02-17	第十次正式发布。 根据购买页面上新“Symantec”和“GeoTrust”证书品牌，更新资料相关内容和描述。
2020-02-10	第九次正式发布。 修改**SCM权限管理**章节中，SCM系统策略名称：“SCM Admin”修改为“SCM FullAccess”，SCM Viewer修改为“SCM ReadOnlyAccess”。
2020-01-20	第八次正式发布。 根据IAM界面变化更新权限管理内容。
2019-10-30	第七次正式发布。 新增**个人数据保护机制**章节。
2019-08-13	第六次正式发布。 修改**SSL证书管理**章节相关内容描述。
2019-05-21	第五次正式发布。 修改**SSL证书管理**章节内容。
2019-02-26	第四次正式发布。 在**与其他云服务的关系**章节中，增加“与Web应用防火墙的关系”。
2019-01-18	第三次正式发布。 修改**SSL证书管理**章节，优化了内容描述。
2018-05-31	第二次正式发布。 增加**与其他云服务的关系**章节。
2018-05-07	第一次正式发布。