天翼云

SSL 证书

用户操作指南

天翼云科技有限公司

1 产品介绍

1.1 产品定义

【摘要】：本页介绍了 SSL 证书产品的基本定义

SSL 证书是用于在 Web 服务器与浏览器以及客户端之间建立加密链接的加密技术，通过配置和应用 SSL 证书来启用 HTTPS 协议，来保证互联网数据传输的安全，全球每天有数以亿计的网站都是通过 HTTPS 来确保数据安全，保护用户隐私。

1.2 产品优势

【摘要】：本页介绍了国产万维信 SSL 证书产品的优势

（1） 万维信 SSL 证书由上海 CA 自主研发，符合国际、国内标准，客户信息和审核数据不出境，全网信任，确保用户信息数据安全；

（2） 一次提交资料，即可支持国际 RSA / ECC、国密 SM2 双算法证书颁发；

（3） 万维信 SSL 证书支持国内 OCSP、CRL 查询，后台服务均通过国内网络优化，确保网络系统运行稳定；

（4） 拥有集销售、客服、技术、研发为一体的原厂服务团队，提供 7×24 小时全年无休

的服务，及时响应用户需求。

1.3 产品功能特性

【摘要】：本页介绍了 SSL 证书产品的基本功能特性

（1）内容加密：建立一个信息安全通道，来保证数据传输的安全；

（2）身份认证：确认网站的真实性；

（3）数据完整性：防止内容被第三方冒充或者篡改。

1.4 应用场景

【摘要】：本页介绍了 SSL 证书产品的一些应用场景

（1）网站数据加密

HTTP 协议无法加密数据，导致网站数据可能产生泄露、篡改或钓鱼攻击等问题。安装 SSL 证书后，网站使用 HTTPS 协议对网站数据的传输进行加密，包括您网站中的企业应用数据、政务信息、支付环节的数据都能实现加密传输，有效保护敏感数据的传输。

（2）网站服务由 HTTP 协议转换成 HTTPS 协议

用户需要将网站服务由 HTTP 协议转变成 HTTPS 协议，可以使用证书服务申请受信任 CA 认证中心颁发的数字证书，然后部署在云平台网站，将 HTTP 访问转换成 HTTPS，为网站访问提供认证加密功能。

（3）提升网站用户访问网站的安全性

如果网站没有安装 SSL 证书，网站地址以 HTTP 开头，浏览器会将此类网站标记为不安全的网站。如果网站已安装 SSL 证书，浏览器会将该网站标记为安全网站，让您网站的用户可以放心访问您的网站。对于已安装 EV 或 OV 证书的网站，浏览器地址栏会展示该网站所

属企业的真实身份，更有效地增强网站用户对该网站的信任，从而提升网站业务的成交率。

（4）CDN 或 SLB 服务上使用 HTTPS 协议

CDN 或 SLB 服务，可以通过 SSL 证书服务将购买的数字证书部署在这些产品中，实现云产品的 HTTPS 化。

2 计费说明

2.1 价格

【摘要】：本页介绍了 SSL 证书产品的价格

加密标准	域名类型	证书种类	证书品牌	周期	销售单价（元）	续订单价（元）
国际标准	单域名	域名型 DV	SHECA 万维信（国产）	年	1078	1078
国际标准	通配符	域名型 DV	SHECA 万维信（国产）	年	5808	5808
国际标准+国密标准	单域名	企业型 OV	SHECA 万维信（国产）	年	10584	10584
国际标准+国密标准	每增加一个单域名	企业型 OV	SHECA 万维信（国产）	年	3834	3834

国际标准+国密标准	通配符	企业型OV	SHECA 万维信（国产）	年	44604	44604
国际标准+国密标准	每增加一个通配符	企业型OV	SHECA 万维信（国产）	年	44604	44604

2.2 试用

【摘要】：本页介绍了 SSL 证书产品的试用规则

OV 证书不提供试用，DV 证书可提供 30 天单域名证书试用，客户可联系电信客户经理协助开通业务试用。

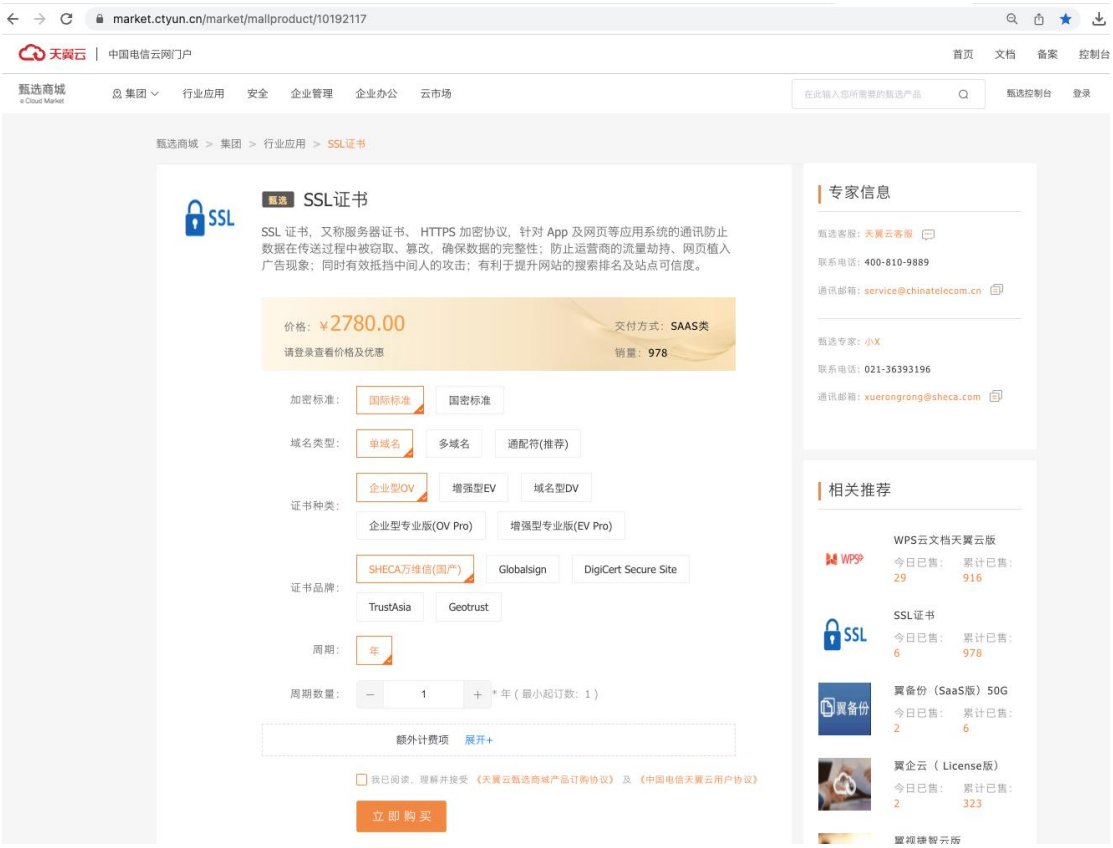
2.3 购买

【摘要】：本页介绍了 SSL 证书产品的购买规则

可以联系电信客户经理在电信 BCP 系统下单，或者直接在天翼云甄选商城进行 SSL 证书产品订购。

甄选商城订购链接：https://market.ctyun.cn/market/mallproduct/10192117。

订购页面如下所示，选择对应证书类型后点击【立即购买】进行订购。



2.4 变更

【摘要】：本页介绍了 SSL 证书产品的变更规则

SSL 证书产品订购后不支持规格的变更，如需变更，请重新进行选购。

2.5 续订

【摘要】：本页介绍了 SSL 证书产品的续订规则

可以联系电信客户经理在 BCP 系统续订，或者在天翼云甄选商城控制台进行 SSL 证书产品续订。如不续订，也可以选择重新订购。续订建议在老证书到期前 1 个月内操作。

注意：续订后新证书签发需要重新做资料审核并重新部署新证书。

2.6 退订

【摘要】：本页介绍了 SSL 证书产品的退订规则

默认不支持退订，如有特殊情况，请联系客户经理。退订需要原路径退订：在甄选商城进行退订，或联系客户经理在 BCP 系统进行退订。经电信内部审核通过后方可退订成功，并且退订操作需在订购 30 天之内完成。

3 快速入门

【摘要】：本页介绍了 SSL 证书产品的分类

SSL 证书根据审核级别不同分为三类，域名验证 (Domain Validation)，企业验证 (Organization Validation) 和增强型验证（Extended Validation）。其具体区别见下表：

产品	DV SSL	OV SSL	EV SSL
信任级别	🔒	🔒🔒	🔒🔒🔒
安全级别	🔒🔒	🔒🔒🔒	🔒🔒🔒
浏览器显示效果	安全 | https://www.sheca.com	安全 | https://www.sheca.com	上海市数字证书认证中心有限公司 [CN] | ...
支持域名	单域名、多域名、通配符	单域名、多域名、通配符	单域名、多域名
审核内容	域名控制权验证	严格的企业身份验证	最高等级的企业身份验证
用途	个人网站及创业型企业	中小型企业、电商	金融证券、银行、第三方支付、、政府机关等
有效期	1年	1年	1年
中文支持	支持	支持	支持
加密强度	支持最高256bit	支持最高256bit	支持最高256bit

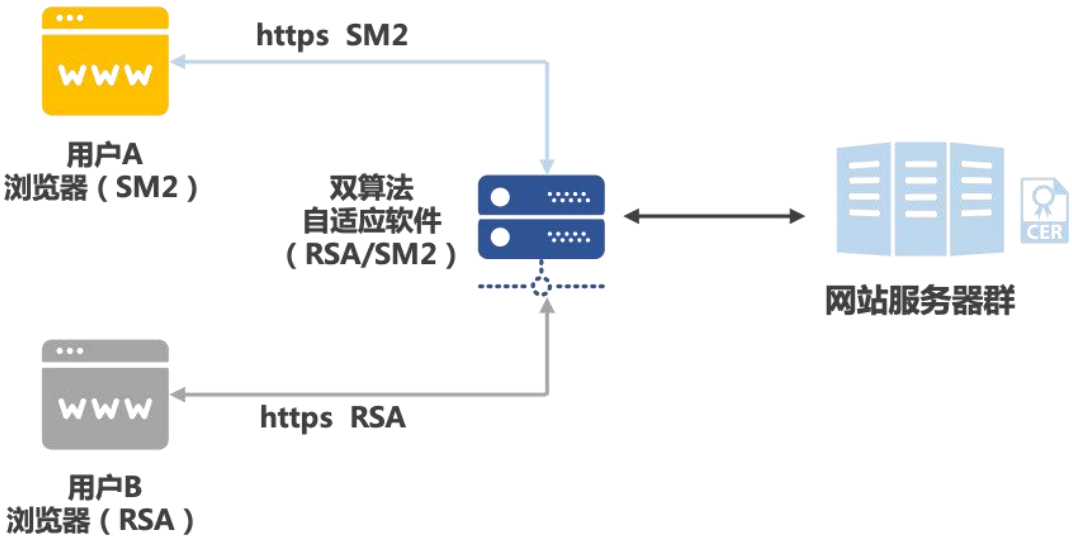
4 用户指南

【摘要】：本页介绍了 SSL 证书产品的使用指南

网站、微信公众号、app 应用、小程序，所有使用 http 协议的地方都可以使用 SSL 证书。特别注意的是，Apple ATS 要求所有 APP 应用的网络请求必须在一个安全（HTTPS）的链上传输，不符合 ATS 要求的应用即将无法在 App Store 顺利上架。小程序要求使用 https 协议的，不然无法正常上架。最新的 HTTP/2 协议中，主流浏览器也仅实现了通过 TLS 加密的 HTTP/2 协议。

万维信双算法证书服务（RSA/SM2 自适应兼容）：

- 向用户提供 SM2 算法 SSL 证书（符合国密要求）和 RSA 算法 SSL 证书（支持全球浏览器和移动终端），兼顾国密合规和全球通用；
- 证书完全基于国内 CA PKI 体系，**无论是国际算法的 RSA2048，还是国产算法的 SM2，根证书都在国内，国产证书完全自主可控。**



5 常见问题

5.1 计费类

【摘要】：本页介绍了 SSL 证书计费常见问题

Q：SSL 可以如何计费?

A：根据所选类型证书，订购成功后即开始计费，具体以电信出账账单为准。注意：证书的使用有效期是以实际审核通过签发之日起开始计算，不以订购日期为准。

5.2 开通类

【摘要】：本页介绍了 SSL 证书开通常见问题

Q：SSL 可以即申请即用吗?

A：由于 SSL 证书根据不同类型，需要进行对应的审核工作，一旦完成审核后，即可部署使用。通常在配合验证的情况下，DV 证书约 1 个工作日，OV 证书约 1-3 个工作日，EV 证书约 3-5 个工作日。

5.3 操作类

【摘要】：本页介绍了 SSL 证书操作常见问题

Q：什么是控制权验证?

A：按规范要求所有的公开可信的 SSL 证书必须完成控制权后才允许签发，控制权验证 CA 机构会协助用户完成，常用的方式有上传指定代码至网站目录下，修改 DNS 记录，邮件验证等方式。

Q：证书私钥丢失后如何处理?

A：证书私钥丢失后可以找 CA 机构重新签发证书，有效期内证书允许不限次免费重新签发。

Q：安卓手机、火狐浏览器提示“不可信任管理机构颁发”、“该证书因为其颁发者证书未知而不被信任”是什么问题?

A：大部分情况下，由于未在服务器上部署中级证书，导致部分客户端如安卓、火狐无法识别 SSL 证书，提示不可信任。解决方法：部署中级证书。

Q：证书什么时候应该进行续期?

A：推荐到期前 1 个月内进行续期，避免影响正常使用。

5.4 使用限制

【摘要】：本页介绍了 SSL 证书使用常见问题

Q：SSL 证书最长有效期是几年？可以签多年么?

A：按照 CA 行业内标准要求 SSL 证书的最大有效期不能大于 13 个月，为了满足用户的需求以及省去不少商务流转环节，我们现推出多年的证书服务，可以咨询商务了解更多详情。

Q：购买的是多域名证书，为什么访问时会出现“此网站出具的安全证书是为其他网站地址颁发的”的错误?

A：多域名证书是用过 SNI 技术实现的，如果您的服务端或用户的客户端不支持 SNI 技术，就可能会出现改错误。

Q：如果服务器换了 IP 地址，原来的 SSL 证书还能用吗?

A：SSL 证书都是绑定域名的，服务器更换 IP 地址没有任何关系，只要域名不变，更换 IP 之后，只需将域名重新解析到新的 IP 地址即可,原来的 SSL 证书当然照样可以用。但如果 SSL 证书是为 IP 地址申请的，则服务器换了 IP 地址，原来的 SSL 证书就不能用了。

Q：能申请 EV 的通配符证书吗?

A：不行，根据规范要求不允许签发 EV 通配符的证书产品。

6 文档下载

6.1 用户使用手册

【摘要】：本页介绍了 SSL 证书产品的使用手册

1. 购买证书

在天翼云甄选商城购买证书，付款成功之后，天翼云账号绑定的邮箱会收到一封订购邮件。

登录地址： https://ctcloud.imtrust.cn/#/user/login

激活码：通过邮件或者天翼云控制台获取

邮件内容如下：

[redacted]

1.登录 天翼云甄选市场后台查看您的订购详情，
具体操作步骤如下:"甄选商城"-->"甄选控制台"-->"我的订单"-->"详情"-->"查看交付单

2.登录"SSL证书管理后台"
SSL证书管理后台 地址: https://ctcloud.imtrust.cn/#/user/login
SSL证书管理后台 激活码 [redacted]

3.补充订单请根据云平台ID，在"SSL证书管理后台"中查询相关记录并点击"补充订单信息"后补充相应的订单信息云平台ID[redacted]

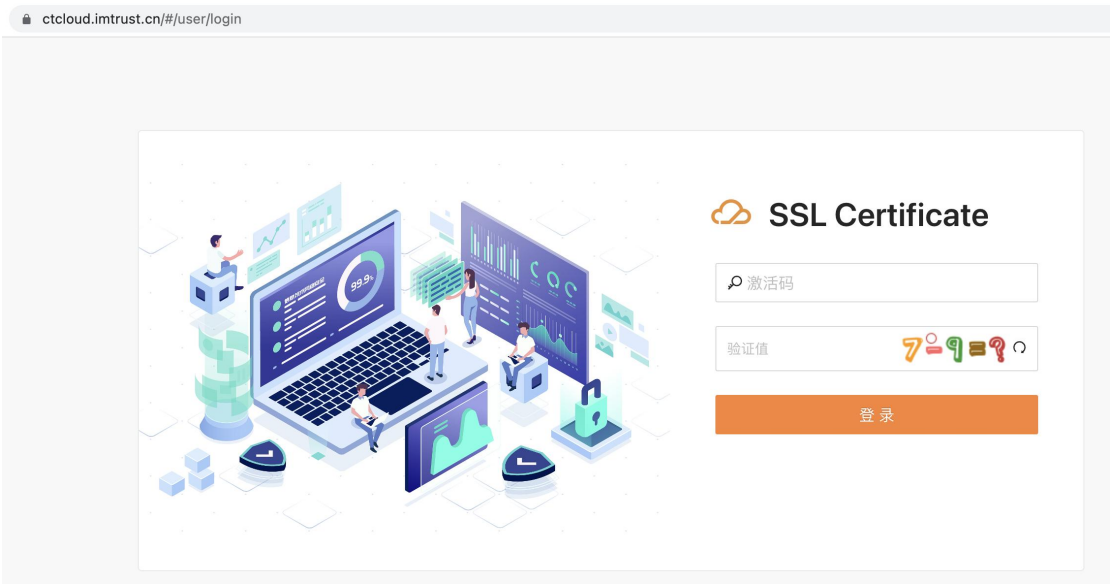
4.等待签发
审核人员将在1-3个工作日联系您天翼云预留的电话进行审核，请注意保持电话畅通!
5.获取证书
在收到订单袋发之后会有邮件通知后，登录管理后台，查询相关的云平台，并点击对应的"订单号，当前页面点击下载证书"即可获取证书!!

如您有任何问题或疑问，欢迎随时和我们联系，谢谢！ wanweixin@sheca.com 或拨打电话 021-36393201 联系我们的支持团队，我们十分乐于为您提供帮助。

2. 登录 SaaS 端界面

使用在天翼云甄选商城控制台或邮件获取的激活码进行登录。

登录界面如下：



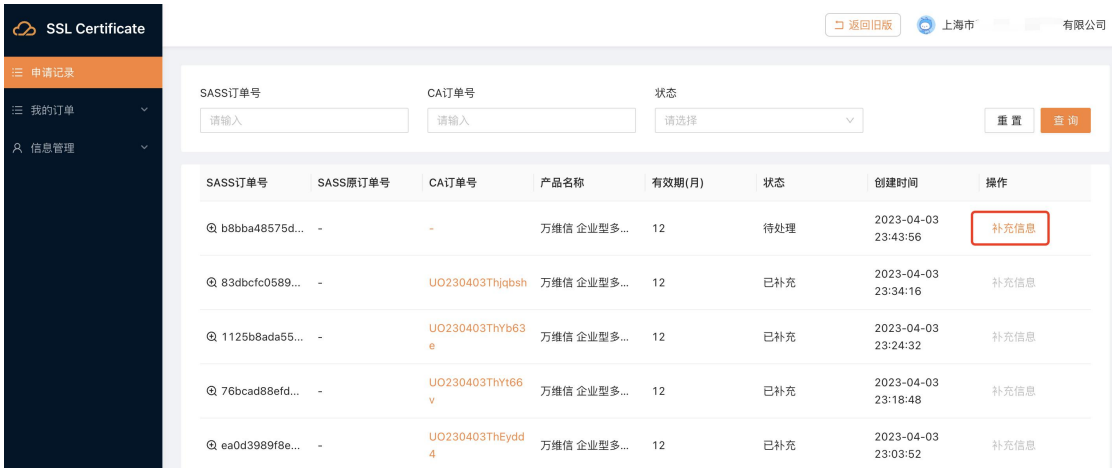
3. 补充信息

3.1 找到关联下单记录

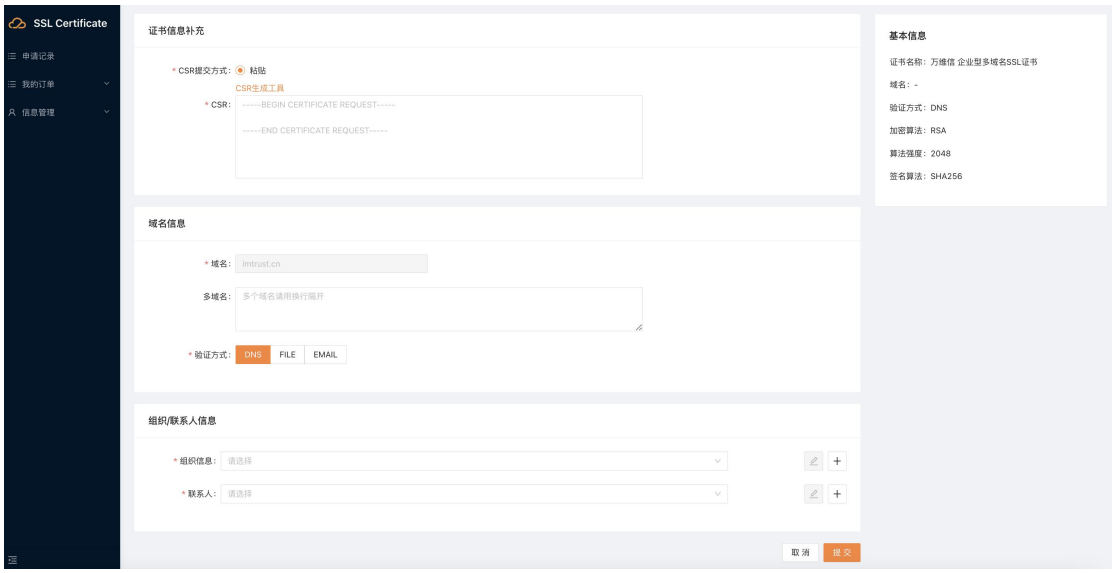
通过云平台的订单 ID，在“我的订单”界面查询到相关购买记录。

3.2 补充订单信息

3.2.1 找到关联记录后点击“补充订单信息”按钮



3.2.2 按照界面上的提示补充表单信息



注意：CSR 的填写可以通过【CSR 生成工具】进行生成，私钥请务必保管妥当，如丢失，只能进行重颁发操作，无法找回；

4. 配合验证

CA 审核人员会及时对客户进行“公司信息“和“域名所有权”的验证，OV 或 EV 客户需要提供相应的文件或者通过年报电话配合审核。

4.1 下载审核资料

如是 OV 或 EV 证书，补充订单后需下载审核资料模板，并完成资料的补充填写。

4.2 上传审核资料

资料进行盖章后，请将盖章资料的扫描件上传至订单平台。

在配合验证的情况下，DV 证书 1 个工作日签发；OV 证书 1-3 个工作日左右签发；EV 证书 3-5 个工作日左右签发。

4.3 域名验证

验证方式可分为 DNS，File，Email 三种，不同证书验证方式稍有不同，具体以订单界面显示为准。验证信息查看方式如下：

请及时完成相应的验证，如验证通过，【验证状态】将更新为【验证完成】。验证完成后请耐心等待证书审核签发。

5. 获取证书

证书签发之后，在订单界面获取证书即可。

6. 证书安装

选择对应的 web 服务类型进行证书安装，如安装过程需要帮助，可联系技术支持：021-36393201。

7 相关协议

7.1 服务条款

【摘要】：本页介绍了 SSL 证书产品的服务条款

SSL 证书产品服务协议

《天翼云 SSL 证书产品服务协议》由用户（“甲方”）与中国电信股份有限公司云计算分公司（“乙方”）共同签订。乙方按照本协议的约定，通过中国电信天翼云官网平台（网址：

www.ctyun.cn）向甲方提供 SSL 证书服务。甲方应当按照本协议约定使用本服务。

甲方使用 SSL 证书服务之前，应当认真阅读本协议的全部内容。甲方点击同意的，视为甲方同意并接受本协议的全部内容，本协议即构成甲乙双方之间有约束力的法律文件。如果甲方不同意接受本协议，请勿使用 SSL 证书服务。

一、定义

1.1 “SSL 证书服务”（以下又称“本服务”）：指乙方提供的 SSL 证书就是遵守安全套接字层协议(Secure Socket Layer)，用来确保 Internet 通信和事务安全的。证书由受信任的 CA 机构，在进行严格的验证后颁发，具有服务器身份验证和数据传输加密功能。

1.2 “管理控制台”是指乙方通过天翼云平台为甲方提供的对其账户已订购产品进行管理、维护的服务系统平台。“管理控制台”是指 http://www.ctyun.cn/vmcontrol/control。

1.3 “甄选商城”是指由乙方提供的天翼云官网之上承载的云办公等应用产品的网络交易平台。

1.4 故障受理：指甲方在使用乙方 SSL 证书服务过程中，出现影响业务使用的情况下，甲方通过乙方提供的客户服务热线进行申告或投诉并得到乙方的回复。

1.5 非故障受理：指甲方在使用乙方 SSL 证书服务过程中，遇到不影响业务使用等情况下，通过乙方提供的客服热线向乙方咨询、申告或投诉并得到乙方的回复。

1.6 响应时间：指自乙方收到甲方咨询、申告或投诉后回复的时间。

1.7 “本网站”或“天翼云平台”：指中国电信天翼云官网平台（网址：www.ctyun.cn）。

1.8 本协议：包括《中国电信 SSL 证书服务协议》正文、附件以及所有乙方已经发布的或将

来可能发布的关于本服务的规则、通知、公告等（统称“服务规则”）。所有服务规则为本协议不可分割的组成部分，与协议正文具有同等法律效力。

1.9 “《用户协议》”指甲方注册本网站账户时与乙方签订的《中国电信天翼云用户协议》。

二、服务内容

2.1 乙方依据本协议约定向甲方提供 SSL 证书服务。本服务的具体内容，以本网站展示并经甲方申请而由乙方实际向其提供的服务为准。乙方有权不断更新服务内容。

2.2 服务前提

为使用本服务，甲方应当首先满足以下全部条件：

（1）同意并接受《用户协议》，已成功注册成为本网站的用户，且在本协议签订时及履行过程中持续拥有合法有效的本网站用户账户；

（2）同意并接受本协议；

（3）按照本网站服务规则申请使用本服务；

（4）按照本协议约定提交相应申请文件且经乙方审核通过；

（5）本协议规定的其他业务使用前提条件。

三、服务费用

3.1 甲方使用本服务，应当按照本协议约定向乙方支付服务费用。

3.2 本服务项下具体服务内容及对应的服务费用，以本网站服务规则及本服务订购页面列明公示的信息为准，甲方可自行选择具体服务类型，并应按照本网站上现时有效的价格体系支

付相应服务费用。

3.3 甲方可使用【账户余额】向乙方支付费用。甲方应保证账户内的余额充足，并在订购本服务、生成订单后，于 48 小时内完成支付。对于逾期未完成支付的订单，乙方有权自行取消。

3.4 甲方购买本服务需要乙方开具发票的，应于订购本服务时，在本网站产品订购界面上申请开具发票，并按格式和要求填写单位、抬头、款项、发票类型及邮寄地址；乙方依法为甲方开具并邮寄相应金额的发票；乙方将在订单支付成功后第 8 日起应甲方要求为甲方开具发票。

3.5 乙方保留随时更新价格及支付方式的权利，更新时将在天翼云官网平台上公告。

3.6 本协议的价格及支付按照甲方订购 SSL 证书服务时约定的价格及支付方式执行。

3.7 甲方对应支付费用有异议的，应当以【书面】方式向乙方提出核对申请。经双方确认核对确有错误的，乙方应对相应费用予以调整。

四、服务开通

4.1 甲方完成订购与 SSL 证书服务关联的云产品后，甲方即可登录本网站，在管理控制台申请开启本服务。

4.2 甲方应保持账户余额充足以确保服务的持续使用。甲方账户余额不足，乙方有权终止为甲方提供服务。

五、用户服务保证

5.1 乙方为甲方提供客户服务的服务热线：400-810-9889。

5.2 乙方为甲方提供客户服务的时间：7 天×24 小时。

六、技术支持保证

6.1 乙方对甲方进行故障受理或非故障受理后，根据具体情况和甲方需求，为甲方提供技术支持保证。乙方工程师服务时间为 7 天×24 小时。

6.2 甲方理解并同意，出于甲方数据及系统安全的考虑，甲方需要乙方工程师直接对其服务器进行 SSL 证书部署操作时，甲方应当以邮件、工单、电话等方式进行授权。甲方应当指定唯一的联系人作为授权人（维护人）并由其在需要时授权于乙方，即只有该授权人有权利要求乙方工程师对其服务进行 SSL 证书部署操作。且乙方仅负责对 SSL 证书服务的运营维护。此外，在授权期间甲方未与乙方工程师沟通，自行进行操作而造成业务不可用等风险，由甲方承担。

七、甲方的权利和义务

7.1 信息的准确性

甲方应承诺并保证在申请证书以及在提供签发该证书所需的相关信息时都要向乙方提供准确、完整、可靠且无误导性的信息。因故意或过失未向乙方提供真实、完整和准确的信息，导致乙方签发证书错误，从而造成相关各方损失的，由甲方承担相应责任。

甲方应声明并确认拥有证书中的电子邮箱地址、主题备用名称里所列的域名或 IP 地址的控制权，如果甲方不再控制电子邮箱地址、域名或 IP 地址，则甲方应及时通知乙方。

7.2 密钥对生成

如果甲方自行生成密钥对，甲方应使用可信赖的系统生成和保护密钥对并满足以下要求：生

成的密钥对密钥长度 RSA 算法不小于 2048 位、ECC 算法不小于 256 位；确保提交给乙方的公钥与私钥正确对应。

7.3 私钥保护

甲方应采取一切合理且必要的措施，以确保能始终控制、不泄漏、妥善保管和通过授权才允许使用证书中公钥相对应的私钥（以及任何相关激活数据或设备，如：密码或 Token）。如甲方保管不善导致数字证书遭盗用、冒用、伪造或者篡改，甲方应当自行承担相应责任。

7.4 私钥的重用

甲方不应使用已经申请过 SSL 证书中的公钥再次申请 SSL 证书。

7.5 防止滥用

甲方应采取适当的网络或其他安全控制措施以防止私钥被滥用，如果存在未经授权访问私钥的情况，则乙方可以直接撤销该证书而无需事先通知。

7.6 证书的接受

在申请人或申请人代表审核并验证证书内容的准确性之前，甲方不得使用证书。在收到证书后的 30 天内未对证书内容提出异议，则视为该证书已被接受。

7.7 证书的使用

证书中公钥相对应的私钥应仅限于甲方本身访问和使用，甲方应对使用证书的行为及其后果负责。所有使用证书在网上交易和网上作业中的活动均视为甲方所为，因此而产生的相应后果应当由甲方自行承担。

证书不得转让、转借或转用。因转让、转借或转用而产生的相关后果应当由甲方自行承担。

在任何情况下，证书都不得用于网络钓鱼攻击、欺诈或对恶意软件进行签名等非法活动及犯罪活动。甲方只允许在证书中主题备用名称里所列的域名或 IP 地址可以访问的服务器上安装 SSL/TLS 或 EV SSL/TLS 证书。

7.8 报告和撤销

以下情况甲方应立即停止使用与证书中公钥相对应的私钥，并向乙方要求撤销证书：甲方的私钥出现可能或事实上的滥用、泄漏、盗用、遗失等任何可能导致甲方对私钥丧失控制权的情况；证书中的任何信息不准确或不正确

7.9 证书使用的终止

甲方应在证书过期或撤销后立即停止使用与证书中公钥相对应的私钥。

7.10 响应能力

甲方应在 48 小时内向乙方回应关于私钥泄露或证书滥用的情况说明。

7.11 承认和接受

如果甲方违反本协议或使用条款，或乙方发现证书被用于非法活动、犯罪活动（如：钓鱼网站攻击、欺诈、发布恶意软件），那么乙方有权立即撤销该证书。

八、 协议期限及终止

8.1 本协议自用户购买或申请开通产品成功之日起生效，至甲方订购服务期限届满时终止，甲乙双方另有约定的除外。

8.2 经双方协商一致的，可提前终止本协议。

8.3 乙方在下述情形下，有权终止本协议：

8.3.1 依据法律法规或政府机关的要求；

8.3.2 乙方认为继续向甲方提供服务将会对乙方造成巨大的经济或技术负担或重大安全风险的；

8.3.3 由于任何法律或政策变动原因造成乙方继续向甲方提供服务不实际可行的；

8.3.4 甲方不按时足额支付相关费用的；

8.3.5 甲方违反本网站《用户协议》的；

8.3.6 甲方不再具备本协议第 2.2 条约定的任一服务前提条件；

8.3.7 甲方违反本协议其他条款的。

8.4 除第 8.5 条约定外，乙方依据本协议约定终止本协议的乙方将按照甲方实际使用天数计算服务费用，将剩余款项（如有）返还，并保留依照法律追究甲方违约责任的权利。

8.5 乙方可提前 30 天在本网站上以发布公告、向甲方发送站内通知或书面通知的方式终止本服务。届时乙方应将甲方已支付的款项（不计息）退还至甲方账户（8.3 除外）。

8.6 如本协议中的任何条款无论因何种原因完全或部分无效或不具有执行力，本协议的其余条款仍应有效并且有约束力。

九、其他

9.1 本协议终止的，不影响甲乙双方之间《用户协议》的效力。若甲乙双方之间《用户协议》

终止，则本协议自动终止。

9.2 本协议未约定的，双方应当同时遵守《用户协议》的约定；本协议与《用户协议》就同一事项存在冲突的，以本协议为准。

9.3 本协议正文与附件具有同等法律效力。如果正文与附件有冲突的，以【协议正文】为准。