目录

产品介绍

金山云证书管理（Kingsoft Certificate Management，简称KCM）与全球各大数字证书颁发及代理机构合作，在云平台上签发通过认证的数字证书，帮助用户网站完成HTTPS化并提供数据安全保障。

产品功能

- **证书签发**：证书在线申请、验证材料一键提交、在线吊销证书等操作，一站式管理实现SSL证书在线购买、审核及快速应用。
- **网站安全**：实现网站HTTPS化，提升数据传输安全等级。

产品优势

- **提升数据安全**：通过HTTPS加密传输数据，防止中间人流量劫持
- **权威CA机构**：Symantec、GeoTrust为用户提供最权威的SSL证书授权服务
- **提升搜索排名**：Google搜索排名会为HTTPS网站加权，辅助站点SEO优化

产品类型

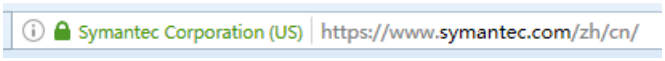
按品牌

名称	介绍
Symantec	赛门铁克是国际知名的高端SSL证书品牌，为全球一百多万台网络服务器提供安全防护，已并入digicert
GeoTrust	GeoTrust是全球第二大数字证书颁发机构
Sectigo	全球知名的高性价比SSL证书品牌
Globalsign	全球最早的数字证书认证机构之一，备受信赖的CA和SSL证书提供商

按等级

简称	说明	特点	审核材料	签发时间	适用对象
DV	简易型SSL证书，仅能对网站传输信息加密，无法验证站点服务器真实身份	价格便宜，申请快捷	提供简单个人信息即可	1-3个工作日	个人网站
OV	标准型SSL证书，即能加密网站传输数据，又能验证网站服务器真实身份	安全性高，审核严格	组织信息、联系人信息、相关营业许可文件	2-5个工作日	电商、教育、游戏等领域
EV	遵循全球统一身份验证标准的SSL证书，目前全球最高等级的SSL证书	安装证书后，浏览器地址栏为绿色且显示公司名字	组织信息、联系人信息、相关营业许可文件	7-10个工作日	金融、支付、网上银行等

关于EV证书地址栏的说明：



按域名数量

名称	解释
单域名证书	可以绑定一个域名
多域名证书	可以绑定多个域名
通配符证书	可以绑定通配符域名，如*.ksyun.com，可以保护无限个**同级**域名（不等于泛域名）
多域名多通配符证书	可以绑多个域名，可额外绑定多个通配符域名（证书至少需要绑定一个主域名）

关于通配符的说明：

颁发给 *.example.com 的单通配符证书可以用于下列域名

```
payment.example.com
contact.example.com
login-secure.example.com
www.example.com
```

由于通配符证书只能覆盖**同级**子域（*不匹配所有子域），该证书无法有效服务于下面的域名：

```
test.login.example.com
```

使用场景

IOS平台应用

从2017年1月1日起，苹果IOS APPLE STORE 将强制平台上的APP通过HTTPS进行加密传输。苹果IOS ATS(App Transport Security)对App的硬性要求：

① ATS要求TLS1.2或者更高，TLS 是 SSL 新的别称。

② 通讯中的加密套件配置要求支持列出的正向保密。

③ 数字证书必须使用sha256或者更高级的签名哈希算法，并且保证密钥是2048位及以上的RSA密钥或者256位及以上的ECC密钥。

目前，已经通过苹果store审核的APP，在2017年1月1号以后如果需要更新版本那么仍需要重新审核，遵循ATS新规。只有浏览器类，影音资源或使用Apple底层网络API及第三方网络库API，调用Safari进程加载页面不需要强制HTTPS。

网站业务

希望通过HTTPS实现加密传输，建议选择DV/OV等级证书。

金融、政府网站业务

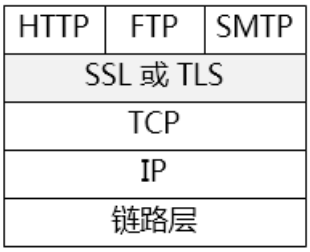
对加密需求较为严格、希望在地址栏中明确标识组织信息，建议选择EV等级证书。

移动端游戏

让App通过HTTPS加密传输，建议选择OV等级证书。

术语说明

- **HTTPS**：即超文本传输安全协议（Hypertext Transfer Protocol Secure）是一种网络安全传输协议。在计算机网络上，HTTPS经由超文本传输协议进行通信，但利用SSL/TLS来对数据包进行加密。HTTPS开发的主要目的，是提供对网络服务器的身份认证，保护交换数据的隐私与完整性。
- **SSL**：安全套接层（Secure Sockets Layer ），及其继任者传输层安全（Transport Layer Security，TLS）是一种安全协议，目的是为互联网通信，提供安全及数据完整性保障。传输层安全协议使用X.509认证，之后利用非对称加密演算来对通信方做身份认证，之后交换对称密钥作为会谈密钥（Session key）。这个会谈密钥是用来将通信两方交换的数据做加密，保证两个应用间通信的保密性和可靠性，使客户与服务器应用之间的通信不被攻击者窃听。



传输层结构

- **SSL证书**：SSL证书通过在客户端浏览器和Web服务器之间建立一条SSL安全通道，即通过它可以激活SSL协议，实现数据信息在客户端和服务器之间的加密传输，可以防止数据信息的泄露。保证了双方传递信息的安全性，而且用户可以通过服务器证书验证他所访问的网站是否是真实可靠。
- **CSR**：Certificate Signing Request的英文缩写，即证书请求文件，用户申请证书时由CSP（加密服务提供者）在生成私钥的同时也生成证书请求文件，用户只要把CSR文件提交给证书颁发机构后，证书颁发机构使用其根证书私钥签名就生成了证书公钥文件，也就是颁发给用户的证书。
- **RSA**：目前最有影响力的非对称公钥加密算法，它能够抵抗到目前为止已知的绝大多数密码攻击，已被ISO推荐为公钥数据加密标准；既可用于加密、又可用于数字签字。RSA算法的安全性基于数论中大整数分解的困难性。
- **ECC**：即椭圆加密算法，一种公钥加密算法，其数学基础是利用椭圆曲线上的有理点构成Abel加法群上椭圆离散对数的计算困难性。与经典的DSA、RSA等公钥密码体制相比，ECC安全性高、处理速度快、存储空间占用小、带宽要求低。

保密级别　对称密钥长度(bit) RSA密钥长度(bit) ECC密钥长度(bit)

80	80	1024	160
112	112	2048	224
128	128	3072	256
192	192	7680	384
256	256	15360	512