

# SSL 证书

SSL 证书，在云上签发各品牌数字证书，实现网站 HTTPS 化，使网站可信，防劫持、防篡改、防监听。

## 证书厂商

### 1、Symantec（赛门铁克）

最老牌的 CA 签发机构，当前所有的银行几乎都是用 Symantec 的品牌，是证书里的玛莎拉蒂，安全性、兼容性及可信度最高，几乎没有出过任何安全事件，是最保险的选择。

### 2、GlobalSign

当前 BAT 三大互联网公司都在用这个证书。

### 3、CFCA

国内的 CA 签证机构，不支持苹果的浏览器，刚在最新的苹果系统上植入的根证书，意味着新的系统支持，老系统的苹果是不支持可信显示的，因此也不推荐，除非是那种对国产化有必需需求的用户才建议选择这个。

## 证书类型

### 1、DV 证书（域名证书）

个人用户，只对域名进行所有权认证，可信度一般。

- 只认证域名的所有权
- 只提供通信链路加密功能

### 2、OV 证书（组织证书）

对组织机构企业信息进行认证，安全性、可信度高，大量企业用户会选择这个。

- 验证域名所有权和申请单位的真实身份。
- 证书中显示申请者的企业单位名称，让访问用户安心使用。
- 提供高强度通信链路加密功能。

### 3、EV 证书（增强证书）

最高可信用度，用户的浏览器端会显示绿色的地址栏，并在浏览器上显示企业信息，建议支付平台、交易网站的域名签发 EV 证书。

- 严格验证域名所有权和申请单位的真实身份。
- 证书在大部分浏览器中能显示绿色地址栏（部分证书在 Safari 浏览器中不显示），有效解决在线信任和网站被假冒问题。
- 证书中详细显示申请者的企业单位信息，让访问用户安心使用。
- 提供高强度通信链路加密功能。

# 保护类型

## 1、通配符域名

保护一个带通配符域名（该\*号同级别的全部明细域名）。

## 2、一个域名

保护一个明细域名。

## 3、多个域名

保护多个明细域名。