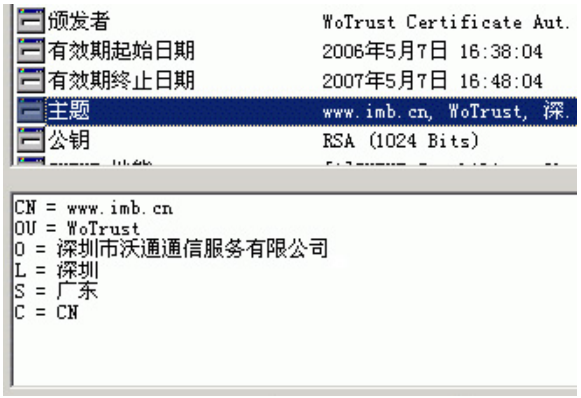
# 第 6 讲 SSL 证书有哪几种？如何正确选择 SSL 证书？

第 5 讲讲到了 SSL 证书有三种：DV SSL 证书、OV SSL 证书和 EV SSL 证书，其实还有一种不常用的 IV SSL 证书。每一种 SSL 证书到底有什么不同？为何会出现这些不同类型的 SSL 证书？本讲详细讲解，并给出了笔者的 SSL 证书选用指南。

## 一、 OV SSL 证书的诞生

Netscape 在 1994 年发明了 SSL 证书，就是现在大家常说的 OV SSL 证书，SSL 证书中含有网站身份信息。笔者在第 4 讲讲 SSL 证书时就展示了 SSL 证书的目的是证明服务器的可信身份，如果服务器不可信，是一个假冒网站，那就应该提醒用户注意网站的身份，以免上当受骗。所以，从这个证书目的出发，SSL 证书的主题信息中一定会有网站身份信息，包括单位名称、所在省市和国家等。笔者电脑中能找到的最老的 SSL 证书如下图所示，证书主题中的 CN 字段(Common Name 公用名称)为网站域名，OU 字段为单位部门名称，O 字段为单位名称，L 字段为单位所在城市，S 字段为单位所在省份，C 字段为单位所在国家。这就是现在的 OV SSL 证书，全名为单位验证 SSL 证书(Organization Validated SSL Certificate, OV SSL)。

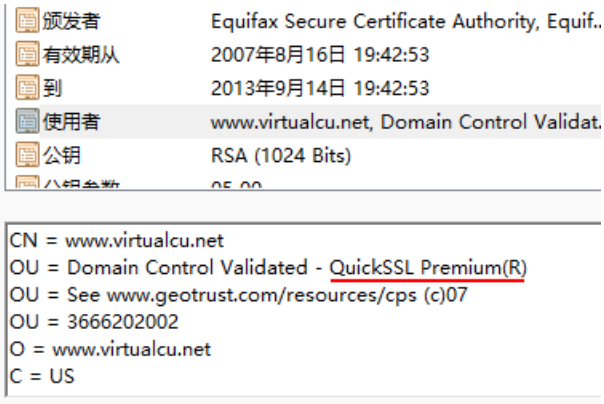




也就是说，SSL 证书发明出来时是只有 OV SSL 证书这一种证书的，那为何现在发展出 DV SSL、IV SSL 和 EV SSL 证书？首先，大家必须明白一个 SSL 证书的签发原则，即 CA 验证了什么信息，才可以在证书主题中显示什么信息，这是 CA 在签发数字证书的基本准则。所以，如果 SSL 证书中包含了网站域名、单位名称和单位注册信息，则 CA 机构一定要验证这些

信息，这就是为何大家申请 SSL 证书都必须完成域名验证，验证网站域名的控制权。其次是 CA 必须验证的网站身份信息，这个需要人工处理，早期全球只有 VeriSign 一家签发 SSL 证书，所以，大家都得等 VeriSign 完成身份认证，VeriSign 需要调查公司的注册信息、电话联系证书申请人核实证书申请信息和申请行为授权等，这就导致了签发一张 SSL 证书需要至少等一周时间。

## 二、DV SSL 证书的诞生

随着 SSL 证书的慢慢普及应用，申请一张 SSL 证书需要一两周时间，这是用户接受不了的，所以 GeoTrust 创始人&CEO Neal Creighton，CTO Chris Bailey 和首席工程师 Kefeng Chen (陈克峰)在 2001 年发明了现在的 DV SSL 证书(Domain Validated SSL Certificate)，自动化完成域名验证后即刻签发 SSL 证书-QuickSSL，这个产品大受欢迎，因为用户再也不用等一周时间才能拿到 SSL 证书了，也是这个产品让 GeoTrust 一举拿下 25%的 SSL 证书全球市场份额。如下图所示，早期的 DV SSL 证书也是从签发 OV SSL 证书的 CA 系统签发，所以仍然保留了 O 字段和 OU 字段，O 字段填写了网站域名而不是单位名称。



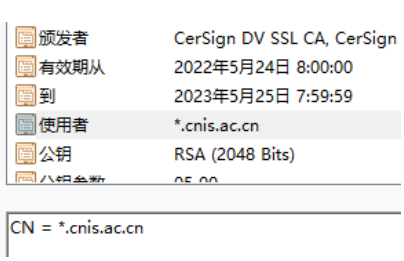


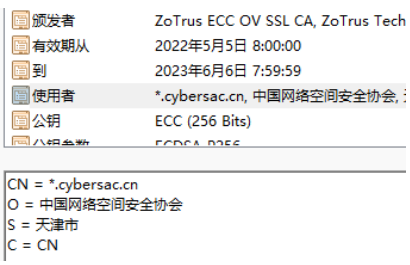
也就是说，GeoTrust 发明了 DV SSL 证书后，SSL 证书就有了两类：验证单位身份的 OV SSL 证书和只验证域名的 DV SSL 证书，而由于 DV SSL 证书可以实现自动化签发，所以不仅可以快速签发而且可以很便宜，甚至可以做到完全免费，这就使得 SSL 证书得到了快速普及应用，因为互联网也同时在全球飞速发展，需要大量的 SSL 证书。

## 三、EV SSL 证书的诞生

随着 DV SSL 证书的普及使用，许多假冒银行网站也能申请到 DV SSL 证书，而浏览器显示 DV SSL 证书和验证网站身份的 OV SSL 证书一样有安全锁标识，这就无法帮助用户准确识别假冒银行网站。为此，CA/浏览器论坛于 2006 年推出了一种新的 SSL 证书类型—EV SSL 证书，英文全名是 Extended Validation SSL Certificate (扩展验证 SSL 证书), 意在更加严格地验证网站的身份，并在浏览器地址栏用绿色来突出显示部署了 EV SSL 证书的网站，绿色就是安全的意思，只要用户上网时看到地址栏变成了绿色，那这个网站就是可信网站！这是 CA 和浏览器产业界最伟大的创新，能非常简单直观地帮助网民识别什么网站是可信网站。最早显示绿色地址栏的浏览器是当时占绝对领导地位的 IE 浏览器，直到 IE 浏览器于 2022 年 6 月 25 日完全退出市场时还是能显示 EV SSL 证书的绿色地址栏。


至此，SSL 证书就有了 3 种，分别是 OV SSL 证书、DV SSL 证书和 EV SSL 证书，这是根据网站的身份认证严格程度分类的，DV SSL 证书最简单，只验证域名所有权或控制权，可以完全自动化签发，所以可以做到免费。而 OV SSL 证书则需要验证证书主题中绑定的单位名称是否合法注册，并同时验证域名所有权或控制权。EV SSL 证书则在 OV SSL 证书验证基础上需要验证申请单位不仅是合法注册的，而且是正常运营中，会验证是单位员工代表单位申请 EV SSL 证书，并且还需签订 EV SSL 证书用户协议，明确确认申请 EV SSL 证书是单位行为，申请证书必须有单位负责人授权签字，CA 需要在验证单位电话号码后联系证书申请人完成电话验证。这三种 SSL 证书的主题信息分别如下 3 图所示，下左图为 DV SSL 证书的主题信息，只显示网站域名，因为只验证了域名；中图为 OV SSL 证书的主题信息，不仅显示网站域名，而且显示单位名称、所在省市和国家。右图为 EV SSL 证书的主题信息，不仅显示网站域名，而且显示单位名称、所在省市和国家，而且还会显示单位注册信息，包括注册号、所在省市和国家、单位注册类型(企业、政府机构、商业机构和非营利机构)。



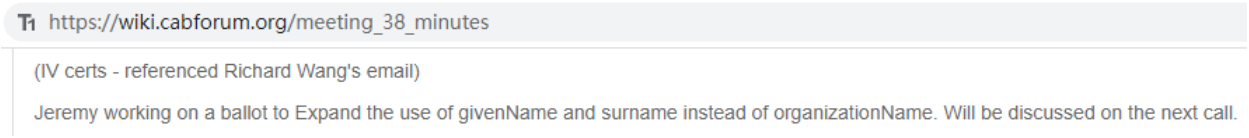




## 四、IV SSL 证书的诞生

随着大量的个人网站也需要部署 SSL 证书，除了可以申请无身份信息的 DV SSL 证书外，个人用户也可以申请 OV SSL 证书来展示其网站的可信身份，则个人姓名只能显示在 O 字段，这显得有点不伦不类，如下左图所示，o＝Richard Wang。为了解决这个问题，笔者在 2016 年 5 月西班牙召开的第 38 次 CA/浏览器论坛工作会议上提出了解决方案，在 SSL 证书国际标准中正式增加一种证书类型：IV SSL 证书 (Individual Validated SSL Certificate)，并增加两个专门的字段 G (Given name，名字) 和 SN (Surname，姓)来显示个人的姓和名，如下右图所示，G=Richard 和 SN=Wang。



笔者联合 DigiCert 的 JeremyRowley 和 StartCom 的 Eddy Nigg 共同发起了 CA/浏览器论坛的第 175 号提案--在 SSL 证书主题信息中增加姓和名字段，提案获得通过，并在随后更新的 SSL 证书标准中体现这次修订，这标志着拥有专用字段的 IV SSL 证书正式诞生，笔者现在对此仍然感到非常的自豪。




至此，SSL 证书就有了现在大家看到的 4 种，分别是 OV SSL 证书、DV SSL 证书、EV SSL 证书和 IV SSL 证书，而由于 DV SSL 证书的免费普及使用，个人用户一般都申请了 DV SSL 证书，所以，大家常见的 SSL 证书就只有 DV SSL 证书、OV SSL 证书和 EV SSL 证书。根据《中国 SSL 证书市场发展趋势分析简报-2022Q4》的统计数据，截止到 2022 年 12 月 31 日的数据，仅验证域名的 DV SSL 证书占比 **83.81%**，验证网站身份的 OV SSL 证书占比 **16.12%**，而扩展验证网站身份的 EV SSL 证书仅占比 **0.07%**。这就是目前的全球 SSL 证书的三种常用的

SSL 证书的签发比例。

导致高达 84%的用户选择 DV SSL 证书的原因有两个：一是免费 90 天的 DV SSL 证书已经实现自动化申请、部署和续期，这是一个一劳永逸的方案而大受用户欢迎，把用户彻底从繁琐的证书申请工作解脱出来；二是常用的浏览器已经不再绿色地址栏特别显示 EV SSL 证书，各种 SSL 证书都是只显示安全锁标识，无法体现 SSL 证书中的身份信息的价值，所以，用户也就是不想费力费钱去申请无法自动化即刻签发的 OV/EV SSL 证书了。

## 五、SSL 证书的分类

前面分别讲了四种 SSL 证书是如何产生的，这是根据网站身份认证方式不同而分类的，有仅验证网站域名控制权的 DV SSL 证书，有验证单位身份和域名控制权的 OV SSL 证书，有扩展验证单位身份和域名控制权的 EV SSL 证书，还要现在不太常用的验证个人身份和域名控制权的 IV SSL 证书。

而根据 SSL 证书绑定的域名类型分类，SSL 证书可以分为单域证书、通配证书和多域证书。绑定一个域名的 SSL 证书称之为单域型 SSL 证书、绑定通配域名(*.domain.com)的 SSL 证书称之为通配型 SSL 证书、绑定多个单域或通配域名的 SSL 证书称之为多域型 SSL 证书。其中 EV SSL 证书不支持通配型，因为无法保证用户不会把通配证书中绑定的扩展验证身份信息用于其他非此身份的子域名网站。上面第三节的截图中第一个是 DV SSL 通配型证书，第二个是 OV SSL 通配型证书，第三个是 EV SSL 证书单域型证书。

## 六、SSL 证书有效期

SSL 证书在诞生时并没有证书有效期的限制，可以是 5 年或者 10 年，但是随着 SSL 证书的广泛使用，特别是 2005 年 5 月 17 日由 VeriSign 和 Comodo 牵头成立国际标准组织-CA/浏览器论坛，出台了一系列 SSL 证书标准，SSL 证书有效期就开始从 5 年缩短到 3 年、2 年、1 年，这是考虑到电脑算力，特别是互联网算力的不断提升，太长有效期的密钥有可能被破解而威胁到 https 加密的安全。

根据谷歌于 3 月 3 日发布的根认证策略的预告，谷歌将推动 SSL 证书的有效期再次缩短到 90 天！意在推动 SSL 证书的自动化部署、提升 SSL 证书的安全性和生态系统的敏捷性，为下一步轻松过渡到抗量子算法的 SSL 证书做准备。估计这个革命性的变化会在今年年底或明年实现，这个动态值得 SSL 证书相关产业包括 SSL 证书提供商和 SSL 证书用户的高度重视。

## 七、SSL 证书选用指南

最后一部分简单讲一下 SSL 证书的选用指南，其实根据三种类型的 SSL 证书签发统计数据已经给出了答案， DV SSL 证书申请量已经占比 **83.81%**，而其中有 80%的 DV SSL 证书都是自动化申请和部署的 90 天有效期的 DV SSL 证书，虽然 CA 机构不愿意看到这个结果，但是这是用户的选择。

笔者给出的建议是：政府网站只需要申请 RSA/ECC 算法的 DV SSL 证书即可，无需提供身份证明材料，这样不仅省钱和快速拿到证书，而且不会出现目前大量存在的政府网站部署的 OV/EV SSL 证书中的 O 字段为公司名称的“错误”证书。而为了国密合规，则必须是部署双算法双 SSL 证书，推荐的搭配是国际 DV SSL 证书和国密 OV/EV SSL 证书，由国密 SSL 证书来体现网站的可信身份。而企业网站可以根据自己的网站特点和品牌知名度来决定选购 DV、OV 或 EV SSL 证书，零信浏览器仍然会绿色地址栏显示部署了 EV SSL 证书或通过 EV 可信网站认证的网站和在地址栏显示单位名称，并且创新地浅绿色地址栏显示部署了 OV SSL 证书的网站和在地址栏显示单位名称。


**下一讲内容预告 | 第 7 讲 浏览器是如何验证 SSL 证书的？**

本讲重点讲一讲浏览器是如何验证 SSL 证书并根据验证结果展示不同的 UI，并讲一下零信浏览器在这方面的创新。

王高华

2023 年 3 月 13 日于深圳

---

请关注公司公众号，实时推送公司 CEO 精彩博文。