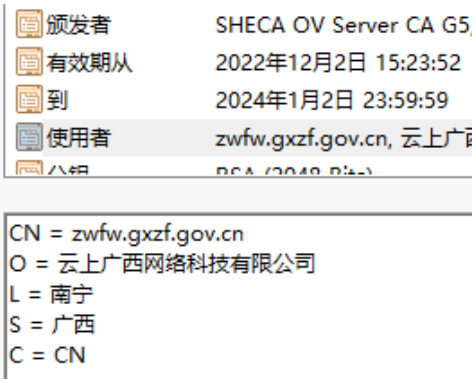
什么是 DV/OV/EV SSL 证书?

本文的 DV 是指仅验证域名控制权的一类 SSL 证书(Domain Validated SSL certificate)，OV 则是验证单位身份的一类 SSL 证书(Organization Validated SSL certificate)，EV 是扩展验证单位身份的一类 SSL 证书(Extended Validation SSL certificate)，本文讲一讲这三种 SSL 证书有什么不同，用户到底应该选择申请哪一种 SSL 证书，并重点讲一讲政府网站应该部署哪一种 SSL 证书，希望本文能有助于在选购 SSL 证书时做出正确的决策。

零信任安全研究院 1 月 1 日发布了《中国 SSL 证书市场发展趋势分析简报-2022Q4》，其中有一段讲的是“关于政府网站部署的 SSL 证书类型”，报告的观点是：对于国际 SSL 证书，我国政府网站**应该只是**申请 DV SSL 证书用于兼容所有浏览器实现 https 加密，没有必要申请需要提供身份认证材料的国际 OV SSL 证书和国际 EV SSL 证书，一方面的确很多政府单位是提供不了身份证明材料，另一方面是除了零信浏览器外的其他浏览器都不再在地址栏显示证书中的单位名称，失去了 OV SSL 证书和 EV SSL 证书能证明网站身份的价值。也正是由于这两个原因导致了大量的政府网站的 OV SSL 证书和 EV SSL 证书中显示的单位名称为企业名称，这显然是非常错误的网站身份信息，不仅完全失去了 SSL 证书能证明网站身份的作用，而且还有可能误导网站访问者。也正是这些原因，我们才认为我国政府网站的国际 SSL 证书应该只申请仅用于加密的 DV SSL 证书。

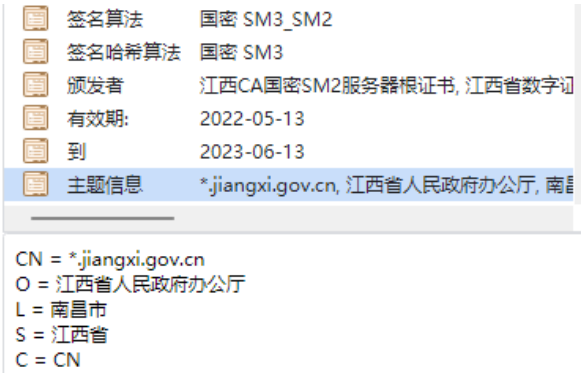
有读者私信我对此观点有不同的看法，所以本文就讲一讲为何我们的报告得出这样的结论。还是先让大家看几个省政府网站部署的国际 OV SSL 证书是什么样子的，毕竟眼见为实。下图中的 4 个省政府门户网站 SSL 证书中绑定的单位名称都是某某公司，这种身份信息已经失去 OV SSL 证书的 O 字段是用于证明网站的真实身份的意义。我们能理解可能是无法要求省政府提供身份证明材料，才不得不用公司的身份证明材料去申请了 OV SSL 证书。笔者对这些政务网站系统集成商给出的建议的是：别再难为政府用户和难为自己了，直接申请一张无需提供任何身份证明材料的 DV SSL 证书即可，无需等待即刻能拿到证书。而现在为政府网站申请的 OV SSL 证书是花钱费力不讨好，本想做好事结果是办成了坏事-“有身份欺诈嫌疑”!



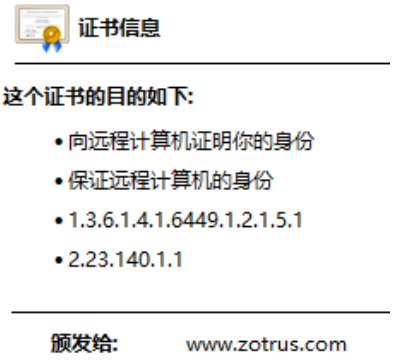
对于以上省政府网站部署的身份不正确的 SSL 证书的情形，当然用户使用其他浏览器都是无法察觉的，因为无论网站部署的是 DV/OV/EV，浏览器地址栏都只是显示一个加密锁标识。而零信浏览器则会读取证书中的 O 字段并显示在地址栏上，那就能让用户马上知道这张证书的 O 字段错了。而为了不能让这些错误的证书身份信息误导用户，零信浏览器已经免费把这些政府网站的真实身份信息写入了网站可信认证库，用户用零信浏览器访问这些网站会显示网站可信认证库中的网站身份信息。

笔者在这里给大家推荐一个典型的 SSL 证书申请案例，还是江西省政府网站，这个网站部署了双算法双 SSL 证书，一张国密 OV SSL 证书，一张国际 DV SSL 证书，国密 SSL 证书的真实身份由国内 CA 验证，完全可以做到不用用户提供任何证明材料，所以建议 CA 机构再

大胆一点，直接写“O=江西省人民政府”即可。而国际 SSL 证书由国外 CA 完成身份认证，要求用户必须提供身份证明材料，这的确有点难为政府用户了，也不知道美国政府用户申请 OV SSL 证书是如何提交身份证明材料的。所以，我们建议就不要难为政府用户了，为用户着想，国际 SSL 证书只申请无需提供任何材料只需验证域名控制权的 DV SSL 证书即可。



可能有些读者会问：同样的是 OV SSL 证书，为何国际 SSL 证书不推荐选用，而国密 SSL 证书则推荐选用？为何不干脆都申请 DV SSL 证书？回答这个问题就要回到为何 SSL 证书要分 DV/OV/EV 了，Netscape 发明 SSL 证书时就是为了证明网站的身份的，大家点开 SSL 证书就能看到 Windows 提示的“这个证书的目的是保证远程计算机的身份”，如下左图所示。刚开始时只有一种 SSL 证书，就是今天的 OV SSL 证书。但是，由于验证网站身份需要时间处理，导致当时申请一张 SSL 证书需要等待一周时间。所以，GeoTrust 发明了自动化验证域名控制权的 DV SSL 证书，使得现在可以随时即刻免费拿到 SSL 证书。但是，随手可得的证书当然会导致欺诈网站也有 SSL 证书，浏览器也会显示加密锁标识(以前称之为安全锁)，让用户无法辨识这个网站到底是验证了身份还是没有验证身份，这就出现了 EV SSL 证书，扩展验证网站身份，所有浏览器地址栏会显示为绿色，并且会在地址栏显示网站的单位名称，如下右图所示。



但是，在谷歌浏览器和火狐浏览器推出自己的免费的 DV SSL 证书后，起市场主导地位的谷歌浏览器就把 EV SSL 证书的绿色地址栏功能给废弃了，他们认为网站只需加密就行了，无论是何种浏览器都只是显示加密锁标识，这直接导致 SSL 证书的双重功能—身份和加密降级为只有加密功能了。这就是为何我们建议只需申请 DV SSL 证书的技术原因。

但是，我国要普及推广国密 SSL 证书，国密 SSL 证书应该牢记 SSL 证书被发明时的初心，SSL 证书能证明网站的可信身份，这是网站的数字身份证，是网站实名备案的数字证明，国密 SSL 证书不能走国际 SSL 证书的重加密轻身份的“歪路”，必须用好国密 SSL 证书能证明网站可信身份的属性用好，因为网站备案后的身份信息只能是网站自己在主页下发自己写上去，而 SSL 证书中绑定的身份信息则是不可假冒、不可篡改的经过浏览器信任的第三方验证的可信身份，这对于建设我国可信的互联网将起到不可替代的巨大作用，能有力促进我国互联网的安全健康发展。

所以，零信浏览器不仅继续让部署了 EV SSL 证书的网站显示为绿色地址栏和显示单位名称，而且对部署了 OV SSL 证书的网站显示为浅绿色地址栏和显示单位名称，这样就能充分发挥 SSL 证书的网站身份证明的作用，体现身份认证的价值。因为网站的可信身份同加密一样重要！

王高华

2023 年 1 月 9 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。