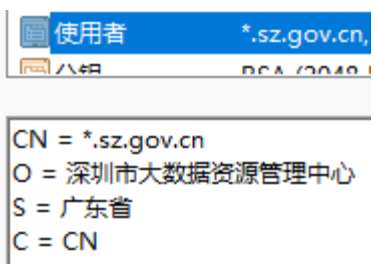
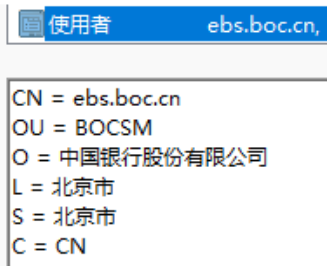
SSL 证书自动化时代的证书选型和方案选择宝典

写这个话题的灵感来自一个 CA 销售人员的求助，他问笔者：我们之前向银行过度吹嘘了 EV SSL 证书的最高安全特性，现在向银行推荐 SSL 证书自动化管理解决方案时发现零信国密 HTTPS 加密自动化网关默认自动化配置的国际 SSL 证书是 DV SSL 证书，银行不干了，担心加密安全有降低，如何同银行用户讲清楚这个问题？笔者认为这的确是一个过度营销的问题，是时候给用户说清楚 SSL 证书在进入自动化管理时代如何选型的话题了，本文绝对值得银行和政府等高端用户认真阅读和收藏，因为这不仅仅是花对钱的问题，更是一个关心加密性能和可靠加密的用户最需要关注的问题。本文意在帮助 SSL 证书用户去恐、解惑、释疑(去 FUD)，认清 SSL 证书的选型误区，在 SSL 证书自动化时代不再纠结证书类型，科学评估并正确选择 SSL 证书自动化管理解决方案。

一、 深入了解三种 SSL 证书类型的不同 — OV/DV/EV

SSL 证书在 1994 年发明时并没有分三种类型，当时的 SSL 证书就是现在的 OV SSL 证书，证书主题中有 O 字段就是 SSL 证书用户的单位名称，这是数字证书应有的特征，因为数字证书是实体单位的数字身份证明文件，当然必须有单位名称。OV 就是单位身份验证 Organization Validated 的缩写，目前全球 SSL 证书市场 OV SSL 证书签发量占比 10.29%。

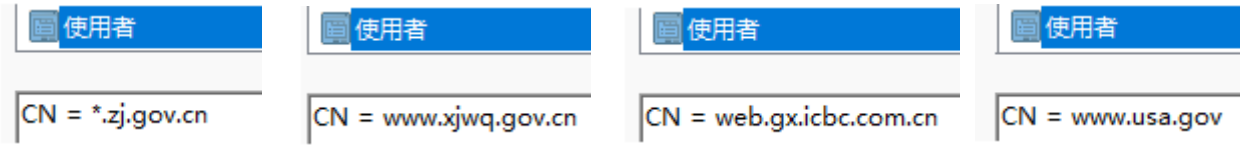




也正是由于 OV SSL 证书需要 CA 完成证书申请单位的身份鉴证，所以需要几天时间才能签发，特别是早期没有公共可信数据库可查，全部需要纸质材料的邮寄送达才能处理证书申请，导致了用户需要等待 1-2 两周才能拿到证书。而随着互联网的快速发展，各行各业都启用了互联网应用，都需要 SSL 证书，但是都忍受不了漫长的签发时间。于是，市场上就出现了 GeoTrust 的 DV SSL 证书—QuickSSL，这是 GeoTrust 发明的只要求用户完成域名控制权验证就自动签发证书，让 GeoTrust 很快就成为了全球第二大 CA，占领 20%市场份额，最后被当时的全球

CA 老大 VeriSign 收购。

DV SSL 证书的主题中没有 O 字段，只有 CN 字段，也就是只有网站域名，因为 CA 只验证了网站域名，没有验证单位身份。这符合 CA 的证书签发原则—验证了什么就显示什么。DV 就是 Domain Validated 的缩写，意思就是仅验证了域名控制权。目前全球 SSL 证书市场 DV SSL 证书签发量占比 90%。



DV SSL 证书由于签发快，并且由于可以实现自动化签发，所以比 OV SSL 证书便宜不少，使得 DV SSL 证书大受欢迎。但是新问题来了，网站部署了 OV SSL 证书和 DV SSL 证书都只是显示加密锁标识，没有什么不同，CA/浏览器论坛就提出了一个改进方案—推出了浏览器显示绿色地址栏和单位名称的 EV SSL 证书，以示区分 OV SSL 证书和 DV SSL 证书。

当然，证书主题信息也增加了公司注册号和注册地信息，CA 必须更加严格地验证 EV SSL 证书的身份信息，就是 Extended Validation (扩展验证)，简称为 EV。这就是 DV/OV/EV SSL 证书的不同，就是证书主题信息不同，CA 验证证书申请单位的身份严格程度不同，浏览器地址栏对部署了 EV SSL 证书的网站显示为绿色地址栏。

但是，2019 年 9 月谷歌浏览器发布了 Chrome 77 版本，不再显示 EV SSL 证书为绿色地址栏，随后火狐浏览器和其他浏览器也同步跟进，所有浏览器都不再显示 EV SSL 证书为绿色地址栏(零信浏览器除外)。这是导致目前全球 SSL 证书市场 EV SSL 证书签发量仅占比 **0.03%**的主要原因，现在基本上只有银行才会申请 EV SSL 证书了。

现在，谷歌浏览器对所有类型 SSL 证书都只显示 tune 标识，其理由是：SSL 证书是用于 HTTPS 加密的，其实所有类型的 SSL 证书的加密强度和安全性能都是一样的，OV SSL 证书和 EV SSL 证书不会给用户带来更多的价值。笔者作为已经从事了 21 年 CA 业务的老 CA 人，虽然不太能接受这个观点，但是现在从一个浏览器厂商的角度来看，也许谷歌是对的，谷歌是

站在用户的利益来考虑的，而不是站在 CA 的利益角度。

二、 HTTPS 加密强度和安全性能与 SSL 证书类型无关，与正确部署有关

谷歌认为“所有类型的 SSL 证书的加密强度和安全性能都是一样的”是否正确呢？我们还是用谷歌浏览器分别访问 3 个部署了 DV/OV/EV SSL 证书的银行网站来做一个比较。如下图所示，第一张截图来自工行官网，部署的是全球最贵的 EV SSL 证书 Secure Site Pro EV，HTTPS 加密所采用的加密算法是 AES_128_GCM。第二张截图来自建行官网，部署的是全球最贵的 OV SSL 证书 Secure Site Pro，可以看出 HTTPS 加密所采用的加密算法是 AES_256_GCM，稍微懂一点密码学的读者一看 128 和 256 就应该知道建行的加密强度更高，但证书是 OV SSL 证书，比工行的 EV SSL 证书便宜不少。再看看第三张截图来自长安银行官网，部署的是最便宜的 DV SSL 证书，HTTPS 加密所采用加密算法也是 AES_128_GCM，加密强度同工行最贵的 EV SSL 证书一样！这里还需要特别指出的是：建行官网网页设计有不安全的表单和其他不安全资源，这个与 SSL 证书类型无关，需要改进页面设计。

相信大家已经从上面的截图充分理解了 HTTPS 加密强度与 SSL 证书类型无关，HTTPS 加密安全其实只与 SSL 证书的正确部署有直接关系，使用权威的 SSL 证书部署体检工具 Qualys SSL TEST 体检发现：工行官网打分为 B 级(及格)，因为没有关闭不安全的 TLS 1.0 和 TLS 1.1 协议，并且没有关闭不安全的 CBC 密钥套件(AES_128_CBC)。建行官网打分也是 B 级，因为不仅没有关闭不安全的 TLS 1.0 和 TLS 1.1 协议，不支持 TLS 1.3，不支持安全协商协议，并且也没有关闭不安全的 CBC 密钥套件(AES_128_CBC)。而部署了 DV SSL 证书的长安银行官网体检打分是 **A-**，仅有一个小问题：不支持 TLS1.3。这个权威的体检结果也有力地证明了 HTTPS 加密安全与 SSL 证书类型无关，只与正确部署有关。笔者在此强烈建议所有 SSL 证书用户都对自己的网站做一次 SSL 证书部署体检，发现部署问题及时修复，一般只需关闭某些不安全的协议即可。

笔者在这里顺便给 SSL 证书用户讲清楚另一个相关的问题，那就是部署通配符证书和多域名证书也是不安全的，因为这两种 SSL 证书都是一张证书一个密钥在多台服务器上共用。一旦某台服务器被黑、或由于管理不善而导致私钥泄露、或 CA 签发错误，则 SSL 证书必须吊销而重新签发，必须重新在多台服务器上去部署证书，这个维护工作量远大于证书的费用，这是得不偿失的证书采购决策失误和证书部署不当。微软云 SSL 证书部署要求通配符证书和多域名证书仅限于在一台物理服务器中的多个网站使用，也就是证书私钥不跨物理服务器使用，这个非常值得所有 SSL 证书用户学习。

三、 要想提高 HTTPS 加密强度和效率，必须选用 ECC 算法和 SM2 算法 SSL 证书

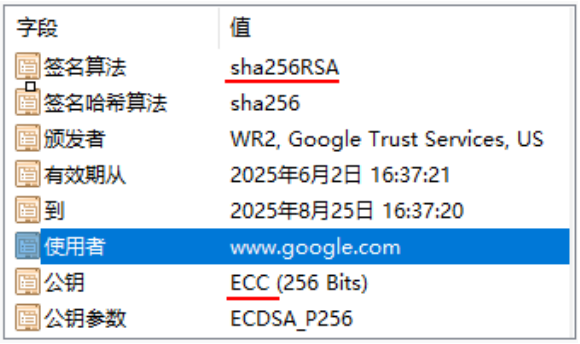
上一段落讲清楚了 HTTPS 加密强度和安全性能与 SSL 证书类型无关，DV/OV/EV SSL 证书都能实现用户所需的加密强度，只需用户在 Web 服务器或网关上正确配置加密套件和其他参数即可。本部分则讲一讲用户如果真想提高加密强度和效率应该怎么做。

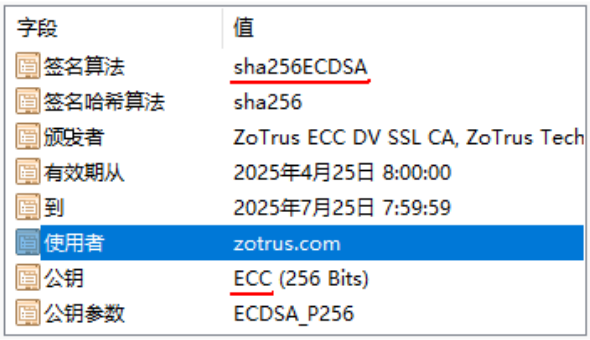
ECC 算法大家都应该不陌生，因为 SM2 算法就是 ECC 算法，只不过 SM2 算法选用了不同的椭圆曲线参数。为什么要用 ECC 算法呢？赛门铁克早在十几年前就做了研究，Apache 服务器部署 256 位的 ECC 算法 SSL 证书对比部署同等加密强度的 3072 位 RSA 算法 SSL 证书，Web 服务器对 ECC 算法的响应速度是 RSA 算法的 18 倍!也就是说,用户访问一个部署了 ECC 算法 SSL 证书的网站只需要 1 秒,而访问一个部署了 RSA 算法 SSL 证书的网站则需要 18 秒！赛门铁克当时的实验用的 Apache 和 IIS 服务器软件，现在流行用 Nginx 服务器软件，性能差距一定更大。

现在银行常用的 SSL 证书是 RSA 算法 2048 位证书，而 ECC 算法常用的是 256 位，其加密强度相当于 RSA 算法 3072 位，也就是说，部署 ECC 算法 SSL 证书比部署 RSA 算法 SSL 证书的加密强度更高，加密效率更高，不仅用户有更好的访问体验，更重要的是用户省电和机房也省电，同时还节省带宽。采用 ECC 算法 SSL 证书实现每次 SSL 证书的握手能节省 1.5K 带宽，对于一个日访问量高达 1000 万次的网站，每天可节省 15G 带宽费用的。工行有一张绑定了 97 个域名的 EV SSL 证书，证书文件比单域名证书将近大一倍，是 ECC 算法单域名证书的 3 倍，再加上中级根证书文件也比 ECC 中级根证书大将近一倍，仅 SSL 协议握手增加的数据大小不同这一项对比，采用 ECC 算法 SSL 证书比采用 RSA 算法 SSL 证书要至少节省三分之一的机房带宽费用，这是一笔可观的节省机房运维费用的技术改进，非常值得普及推广。从这个角度来讲，也能证明选购多域名证书也是一个错误的选择，因为多域名证书文件必须单域名证书文件大了不少。

所以，真正能提高 HTTPS 加密强度的是改进密码算法，改用 ECC 算法和 SM2 算法 SSL 证书，这就是为何我国商用密码算法采用 ECC 算法而不是 RSA 算法的根本原因，也是目前各大国际互联网巨头官网都纷纷采用 ECC 算法 SSL 证书的根本原因，加密强度高、响应快、省流量、省电、环保、省钱。

但请注意：目前市场上的 ECC 算法 SSL 证书有两种，一种是从顶级根、中级根到用户证书都是 ECC 算法的全链 ECC 算法 SSL 证书，另一种是只有中级根和用户证书才是 ECC 算法的 SSL 证书，或者只有用户证书才是 ECC 算法，这三种情况虽然 HTTPS 加密性能是一样的，但是 SSL 握手流量是不一样的，并且差别很大。同时，还要注意的是 ECC 算法根证书是否足够老，越老的根证书通用性越好。如下左图所示，谷歌官网部署的是 ECC 算法 SSL 证书，但中级根和顶级根仍然是 RSA 算法证书。如下右图所示，零信官网部署的顶级根、中级根和用户证书都是 ECC 算法是全链 ECC 算法 SSL 证书。





四、 关于 SSL 证书品牌的选择，多供应商才是关键

采购任何产品选择大品牌或第一品牌是一个明智的选择，如果不用考虑经费有限的话。但是，选购 SSL 证书就不适用这个常规选择，因为 SSL 证书供应链非常不稳定。SSL 证书这个产品非常脆弱，其价值完全取决于四大浏览器特别是已经占领 70%全球市场份额的谷歌浏览器是否信任。

俗话说“枪打出头鸟”，这是古人的智慧，在 SSL 证书市场非常适用。全球第一大 CA-赛门铁克于 2017 年 12 月所有旗下品牌 SSL 证书都遭遇谷歌浏览器不信任，曾经的全球第二大 CA-Entrust 所有品牌 SSL 证书在去年 12 月遭遇谷歌浏览器不信任，本月 31 日谷歌浏览器不再信任台湾第一大 CA-中华电信 CA 的 SSL 证书。相信所有银行用户都应该还记得当时紧急替换赛门铁克 SSL 证书的通宵达旦加班的痛苦，全球两百多万个赛门铁克 SSL 证书用户都应该记得那个至暗时刻。

所以说，选择 SSL 证书品牌不能只选择第一品牌，明智的选择还是“不把鸡蛋放在一个篮

子里”，应该同时选择多家 CA 不同品牌的 SSL 证书，不要只认一家 CA 机构，关键系统域名应该选用多家 CA 机构的 SSL 证书，这样才不会出现一旦某个 CA 出问题了，需要手忙脚乱去重新申请 SSL 证书。因为谁也无法保证，明天太阳出来时，又是哪一个倒霉的 CA 被谷歌浏览器不信任了。

但是，如果是传统人工部署方式，这个多供应商策略不仅增加了 SSL 证书采购费用，也只是稍微缓解了 SSL 证书断供隐患，并没有解决被恶意吊销问题，更没有解决仍然需要人工申请和部署才能不影响业务系统的 HTTPS 加密难题。只有实现了 SSL 证书自动化管理，并且能自动切换 SSL 证书供应链，才能真正保障 SSL 证书供应安全。

五、 SSL 证书自动化时代，最佳双算法 SSL 证书选型是国际 DV+国密 OV

随着 5 月 16 日逐步缩短 SSL 证书有效期的国际标准的落地，SSL 证书强制进入自动化管理时代，这是所有网站特别大型机构面临的紧急难题，如工行就已经申请了 8 百多张国际 SSL 证书，其他银行也不少。SSL 证书有效期将缩短为 47 天，有多个网站系统需要部署 SSL 证书的单位必须现在就开始规划 SSL 证书自动化管理解决方案了，SSL 证书选型也就面临新的选择问题。

在人工申请 SSL 证书和人工部署 SSL 证书时代，如果单位经费充足，申请 OV SSL 证书和 EV SSL 证书能让专业用户看到证书主题中有单位名称，这是唯一的优点，并不存在加密强度更高的虚假宣传特点。但是，现在已经进入 SSL 证书自动化时代，必须实现 SSL 证书的自动化申请、自动化完成验证、自动化签发和自动化部署。而我国关键信息基础设施运营单位必须实现双算法(SM2/RSA)SSL 证书的自动化管理。

而要想实现 SSL 证书的自动化管理，也只有 DV SSL 证书能承担此重任了，因为只有 DV SSL 证书才能实现自动化文件验证后自动化实时签发，这样即使将来进一步缩短 SSL 证书有效期，哪怕是缩短为一天，也不是问题。所以，SSL 证书自动化管理解决方案的最佳方案是自动化签发 DV SSL 证书，而不是 OV/EV SSL 证书，当然也正是因为 HTTPS 加密强度与 SSL 证书类型无关，所以用户无需担心会影响网站安全性能，美国政府官网部署的就是自动化更新的免费 DV SSL 证书。

对于必须满足国密合规和全球信任的要求的网站，需要自动化配置双算法 SSL 证书，国际 SSL 证书当然只需配置 DV SSL 证书即可，这样不仅能实现自动化签发和自动化部署，还能满足这些关键信息基础设施网站的运营单位的身份鉴证数据不出境的要求，因为 DV SSL 证书无需证书申请单位提供任何身份证明材料。自动化配置的国密 SSL 证书当然也是首推 DV

SSL 证书，以便无需 CA 审核而自动化完成国密 SSL 证书的申请、验证和部署。

零信技术双算法 SSL 证书自动化管理解决方案是一个端云一体的解决方案，“端”是一个硬件产品--国密 HTTPS 加密自动化网关，默认自动配置的国际 SSL 证书是 ECC 算法 DV SSL 证书，这是考虑到 ECC 算法比 RSA 算法加密强度更高，响应更快、更省电和更省带宽。并且这张 ECC 算法 SSL 证书是全链 ECC 算法，属于单域名证书，而不是不安全的通配型和多域型证书，是最安全的“一站一密钥一证书”部署方式，证书密钥不出网关硬件，保证了密钥安全。HTTPS 加密算法是 AES_128_GCM，按照最严格的国际标准自动化部署证书，Qualys SSL 体检都是 **A+**。零信网关默认自动配置的国密 SSL 证书不是 DV SSL 证书，而是 OV SSL 证书，但也是自动化实时签发的。这是由于零信云 SSL 服务系统联合上游 CA 系统通过自动化获取用户配置的网站域名的工信部 ICP 备案数据，并以此身份数据为可信的第三方数据源在自动化完成域名验证后自动化签发了国密 OV SSL 证书，满足用户需要 OV SSL 证书的需求，为用户提供更超值的国密 SSL 证书。

零信技术双算法 SSL 证书自动化管理解决方案的“云”就是零信云 SSL 服务系统，为零信网关提供双算法 SSL 证书的自动化签发服务，已经对接了多家国际 CA 和多家国密 CA，实现了自动切换双算法 SSL 证书供应链，确保了无论那家 CA 无法供货时都可以可靠地为用户网站自动化签发国际 SSL 证书和国密 SSL 证书，切实保障了网站 HTTPS 加密的不中断可靠运行。

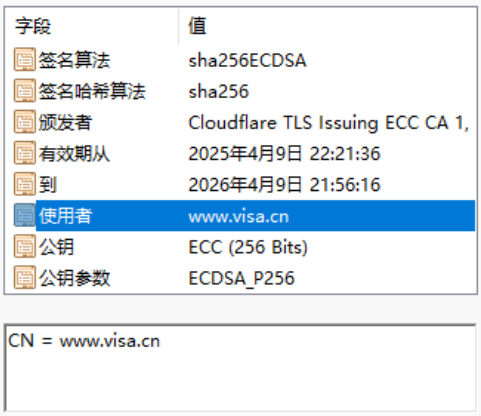
六、 评估 SSL 证书自动化管理解决方案时还需要考虑什么？

SSL 证书从人工管理到自动化管理，这是 2026 年 3 月 15 日即将到来的一次 HTTPS 加密技术革命，是每个网站运营者必须要做的升级改造工作。而这次技术革命的最终目的还是为了应对下一个将于 2029 年 12 月 31 日到来的 HTTPS 加密从传统密码到抗量子密码的技术革命，这次技术革命也要求所有网站运营者必须升级改造系统以支持后量子密码。

所以，所有网站运营者在规划本次 SSL 证书自动化管理解决方案时应该同时考虑下一步 3 年内还要做的技术改造—支持后量子密码，最佳解决方案是本次 SSL 证书自动化管理升级改造能同时完成下一次的 HTTPS 加密抗量子密码技术改造，从而节省两次的改造费用，确保业务系统能无缝升级到抗量子密码时代，轻松应对现在和将来的 HTTPS 加密安全威胁。

请大家看一个 Visa 官网的证书部署案例，如下左图所示，其官网已经实现了后量子密码(ML-KEM768)混合密钥协商机制的 HTTPS 加密，而部署的 SSL 证书就是一张 ECC 算法的 DV SSL 证书，如下右图所示，而不是国内银行普遍使用的 RSA 算法 EV SSL 证书。这才是最安

全的部署方案，完全符合笔者在上面列出的 SSL 证书类型选型和 SSL 证书自动化解决方案选型的全部要求，值得国内银行借鉴和学习。



七、 SSL 证书自动化时代，不选证书类型，只选 SSL 证书自动化管理解决方案

SSL 证书是一个实现 HTTPS 加密所必需的产品，现在已经进入了 SSL 证书自动化时代，标志着人工选购和人工部署 SSL 证书的时代已经结束，进入了一个只需选择 SSL 证书自动化管理解决方案的时代，所以本证书选型宝典也是对上一个时代证书选型的总结，无论是选对了还是选错了都不再重要，重要的是将来的证书自动化方案必须选对。

评估一个 SSL 证书自动化管理解决方案是否适合于自己的业务系统，必须结合 SSL 证书的选型经验和教训，从以下七个方面去综合评估，只有评估得分 90 分以上才是可选的好方案。

(1) 解决方案中自动化配置的 SSL 证书类型(DV/OV/EV)不是第一考量的因素，SSL 证书品牌也不是第一考量的因素，第一考量的因素是现有业务系统是否需要重构，改动大不大，是否会影响业务系统的正常运行，最终用户是否受影响。优先选择微改造方案，优先选择不中断业务和不影响最终用户的无缝升级方案。评估占比 25 分。

(2) 必须是双算法 SSL 证书的自动化管理解决方案，不能走国际 HTTPS 和国密 HTTPS 加密建设两套独立系统的老路子，必须同时直接支持双算法 SSL 证书自动化管理，这样就可以把老的两套系统方案一同改造为一套系统，降低系统复杂性，提高系统可靠性。评估占比 20 分。

(3) 必须检查证书自动化管理解决方案是否支持多 CA 自动签发双算法 SSL 证书，绝对不能是单一 CA 签发证书，否则一旦这家 CA 出问题，自动化仍然是空谈。这一点非常重要，必须要求双算法 SSL 证书支持多通道自动切换签发，并且可选优先默认签发 CA。评估占比 15 分。

(4) 必须评估 SSL 证书自动化管理解决方案是否支持无缝升级到抗量子密码的 HTTPS 加

密自动化，并且是否是免费升级支持。评估占比 15 分(免费支持得 15 分，收费支持得 10 分，不支持得 0 分)。

(5) 必须要求国际 SSL 证书采用 ECC 算法 SSL 证书，最好是全链 ECC 算法，这不仅节省机房电力和带宽而省钱，而且能大大提升用户体验。评估占比 10 分(全链得 10 分，非全链得 5 分，不支持得 0 分)。

(6) 必须检查自动化配置的双算法 SSL 证书是否实现了每个网站独立密钥和独立证书，并且必须检查 SSL 体检是否达到 A 级。评估占比 10 分。

(7) 必须同时把 WAF 防护改造一并考虑，因为所有 Web 应用都需要 WAF 防护，这就要求双算法 SSL 证书自动化管理不能落下 WAF 防护。评估占比 5 分。

王高华

2025 年 7 月 28 日于深圳
