CSC

SSL 发展态势

洞悉证书管理，制胜关键转型

摘要：SSL 发展态势不断演变，碎片化管理可能会让企业蒙受巨大损失。

随着安全套接字层 (SSL) 证书续订周期缩短，企业不能再拖延向证书自动化验证的过渡。同样，企业也无力承受因碎片化 SSL 管理方式而使域名安全受损的风险。

域名安全领域即将步入前有未有的变革时期，若应对不当，企业在保护在线品牌和数字身份方面可能会远远落于人后。尤其值得注意的是，WHOIS 电子邮件地址验证已于今年早些时候停用，而且从 2026 年 3 月起，证书有效期和域名控制验证 (DCV) 复用周期将会缩短，这些都将深刻改变企业的运营模式。

到 2029 年，SSL 和传输层安全 (TLS) 证书的有效期将从 367 天大幅缩短至仅 47 天，这意味着习惯了一年一续的企业今后每年需完成近八次的证书续期。此外，到 2029 年，DCV 复用周期也将从 367 天缩短至仅 10 天。

这些变革恰逢低成本、易获取的域名验证证书主导市场之际。

网络犯罪分子利用这些廉价或免费的证书来仿冒各类品牌，使其欺诈网站看上去真实可信，进而诱骗用户点击恶意链接并窃取用户数据。

与此同时，一些企业对安全问题愈加重视，但我们的年度《域名安全报告》指出，有很大一部分企业仍然面临严重的域名安全风险。我们的研究发现，超过三分之二的全球 2000 强企业落实的安全措施不到建议措施的一半。

在本《SSL 发展态势》报告中，我们分析了与 240 万个域名相关联的超过 80.2 万个数字证书的使用趋势与模式，以期了解企业如何监管 SSL 证书及其对域名完整性保障的影响。通过调研以及与企业高管的直接交流，我们发现企业对于 SSL 证书生命周期和 DCV 重用周期缩短的战略应对普遍存在忽视或延迟实施的现象。本报告将深入剖析这些问题，并提出规避风险的必要措施。

太多品牌选择了更易获取的证书

SSL 证书通过验证证书凭据，并加密网站服务器与用户浏览器之间的连接，来确认在线品牌的合法性与安全性。

SSL 证书具备两大核心功能：

- **安全：**通过加密来保障登录凭据、信用卡号和其他敏感数据的安全。
- **信任：**用户相信持有证书的网站是由合法实体运营，且数据传输安全可靠。身份验证级别随证书的验证级别而变化。

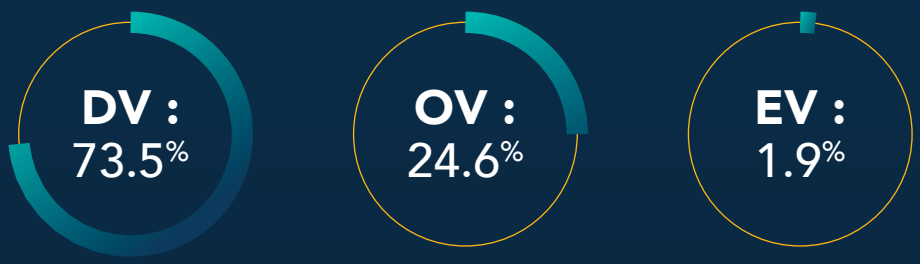
但我们的研究表明，这种理想的安全和信任状态并非常态，绝大多数在线品牌倾向于选择更易获取的证书类型，以减少工作量并提升效率。

SSL 证书验证有三个级别：

- **域名验证 (DV)：**DV 证书成本较低，获取速度最快。DV 仅验证证书购买者对域名的控制权。任何域名注册人均可获得 SSL 证书，无论其域名使用意图如何。
- **组织验证 (OV)：**在 DV 的基础上，OV 还会对组织的特定信息进行验证，例如商业登记证书。
- **扩展验证 (EV)：**EV 证书的验证流程最为彻底、严格，通过对组织的法律资质、实体存在及运营状况进行深度核查，提供更高的安全保障。

我们研究发现，DV 证书占证书总数的近四分之三 (73.5%)，OV 证书占近四分之一 (24.6%)，而 EV 证书占比不足 2% (1.9%)。

证书类型分布情况：

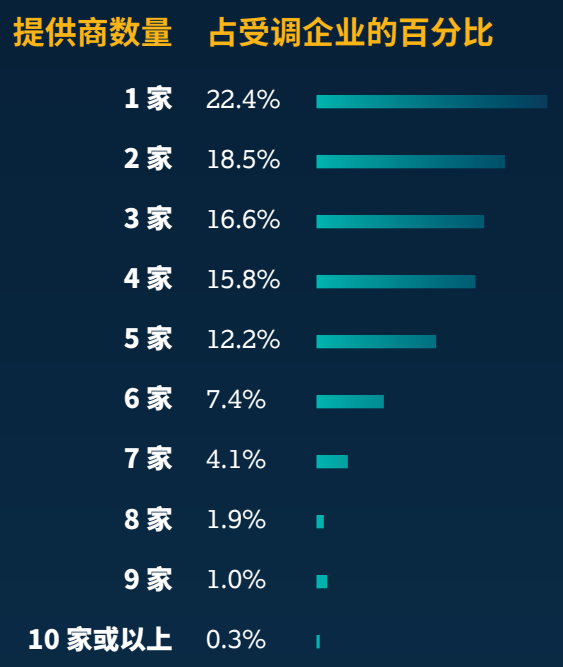


从分布情况来看，DV 证书是最受欢迎的，这并不令人意外，因为它们购买更便捷。当企业采用提供此类低成本证书的供应商时，网络犯罪分子也能通过同一供应商获取同类证书，为欺诈网站披上“合法”外衣，并通过附加的超文本传输安全协议 (HTTPS) 获取用户信任。欺诈者的手段日益复杂，远非昔日那些靠错字和错误语法来仿冒网站的伎俩可比。恶意行为者十分善于伪装自己，而 DV 证书的易获取性只会助长他们变本加厉地冒充合法企业。

过去，使用 EV 证书的网站会显示绿色地址栏，以此向访客表明该网站受经过全面验证的组织保护。后来，主流浏览器不再支持绿色地址栏，EV 证书的采用率亦随之下降。

这些数据引发了若干疑问：针对每种类型的网络资产应获取哪种证书，IT 部门是否制定了明确的策略？还是说仅仅因为“获取简单快捷”就选择了 DV 证书？

采用的提供商越多，风险点就越多



我们的研究表明，近 **60% 的企业**使用三家或以上的证书提供商，其中有一家企业的提供商甚至有 13 家之多。

上图显示，绝大多数企业采用不止一家证书提供商。

事实上，约 60% 的企业使用三家或以上的提供商，这可能会给管理带来诸多不便。这可能会导致管理不集中、流程分散、效率低下——随着证书生命周期和 DCV 复用周期缩短，不良影响将“呈指数级”增长。

整合到单一提供商可显著加快证书续期速度并提高故障排除效率。若出现 SSL 相关问题，安全团队成员只需对接一家提供商即可解决问题。

此外，与单一提供商合作可以降低风险。与其为了应对不同的续订截止日期，疲于对接多家提供商，不如只选一家可靠的提供商，确保及时接收续订通知。同时管理多家提供商还可能会丧失整合到单一提供商所能带来的成本效益。

主流提供商并非企业级提供商

排名前三的证书提供商：

Let' s Encrypt、Google® 和 Amazon®

合计占比：占受调企业证书的 66%

受调企业的 DV 证书绝大多数 (89%) 来自这三家提供商。它们提供的低成本方案对寻求降本的企业具有一定吸引力，但另一方面，CSC 维权团队所关停的欺诈性域名的证书也主要来自这些提供商。证书的易获取性在吸引合法企业的同时，也同样为恶意行为者大开方便之门。

CSC 所关停的欺诈性域名的主要证书提供商：

- Google
- Let's Encrypt
- Cloudflare®
- Amazon

为了节省成本和提高效率，企业往往会选择这些消费级提供商。然而，这些提供商无法提供企业级支持，无法帮助企业应对即将到来的 SSL 行业变革。随着证书续订周期逐步缩短，这种短视做法还会带来不必要的麻烦。

在证书有效期缩短至 47 天前的窗口期，企业必须做好准备工作，不容忽视或拖延。若拖至最后一刻，等待在面前的将是极其棘手和混乱的转型局面。日益频繁的证书续期和 DCV 可能会让企业应接不暇。错过续订可能会导致整个域名和应用程序瘫痪——而它们是业务运营的关键基石。

若能提前规划，并寻求企业级 SSL 证书提供商的支持，便可避免在慌乱应对中付出高昂代价。成熟的合作伙伴不仅能提供积极有效的证书策略，还能提供自动化工具，以取代耗时的手动流程，确保因证书过期导致中断的情况绝对不会发生。借助此类工具，代理可以通过自动化续订流程完成证书的申请、接收和安装。

但将自动化工具集成到系统中需要一定时间。这并非“即买即用”的解决方案，因为其中涉及诸多细节问题。例如，现有的系统组件可能与工具不兼容，这意味着企业需要更换组件。正因如此，忽视或推迟应对日益加快的续订周期将导致代价高昂的混乱局面——而这本可避免。

实现最佳自动化的三个步骤

为避免因证书过期导致服务中断，企业日益认识到，必须依靠自动化来管理 SSL 证书。过去，他们尝试通过手动方式操作，即用电子表格跟踪到期时间，以一年一续的方式管理证书。但行业变革势在必行，自动化成大势所趋。

如前所述，自动化集成并非易事。同时采用多家证书供应商以及管理过程中的疏漏都会导致企业陷入瓶颈，加剧复杂局面。为确保顺利推进自动化集成，我们建议采取以下步骤：

规范流程并形成文档记录。

团队成员流动频繁，事物瞬息万变。但无论如何，都需要为证书管理建立一套持久稳定的标准化流程。在推进自动化集成之前，请务必制定好相关实践规范并形成文档记录，以便当前及未来的团队成员有章可循。在文档中记录推进过程中遇到的痛点，使团队成员了解过去出现的问题及解决方法。

培训自己和所在团队。

在实施自动化流程之前，需要理解当中涉及的诸多要素。与单一、成熟的证书提供商合作对学习过程大有裨益，因为这类提供商对这些要素了如指掌，并能为客户提供相应培训。

例如，单一提供商可以帮助客户决定是购买“大型自动化解决方案”，还是选择成本更低、更务实的方式。市面上有许多 IT 工具（包括开源工具和基于供应商应用程序接口设计的工具）可以作为单一大型解决方案的替代选项。高资质的提供商能帮助客户做出明智决策。

涵盖所有环节。

在开展自动化集成工作时，团队有时会遗漏某些内容，这是错误的做法。“头痛医头，脚痛医脚”的做法必然会留下明显漏洞，成为集成道路上的绊脚石，因此必须涵盖完整的工作流程。

结论

证书无处不在，各企业的运营都离不开它们。客户只要看到“网站不安全”的弹窗警告，就会立即转投竞争对手的怀抱。然而，大多数企业对自己持有的证书缺乏有效管控。行业变革如期而至，企业不得不部署自动化，并为此做好充分准备。

证书生命周期和 DCV 复用周期双双缩短，网络行业弥漫着“山雨欲来”的气息——那些迟迟不为证书续期做规划的企业将在仓促过渡中面临更高的成本与风险。而选择与一家可靠的证书解决方案提供商合作，着手整合工作，则能借助自动化技术，实现更平稳、更安全的过渡。

CSC 的数字证书管理解决方案套件灵活性强，并可为不同需求的企业提供定制化服务，欢迎了解详情。

联系我们 +86 21 63913188 | cscdbs.com/cn

CSC 简介

CSC 是值得信赖的优选安全和威胁情报提供商，深受福布斯全球企业 2000 强和全球最佳品牌 100 强 (Interbrand®) 企业的青睐，专注于域名安全和管理以及数字品牌和欺诈防护业务。随着全球越来越多的公司加大投资力度完善安全状况，我们的 DomainSec℠ 平台可以一展身手，帮助这些公司了解他们存在的网络安全漏洞并且保护其在线数字资产和品牌。企业可以凭借 CSC 的专有技术来增强自身的安全状况，防范针对其在线资产和品牌声誉的网络威胁，从而避免遭受严重的收入损失。CSC 还提供在线品牌保护（将在线品牌监控和维权活动相结合），多维度审视防火墙外针对特定域名的各类网络威胁。欺诈防护服务可在攻击的早期阶段打击网络钓鱼，使我们的解决方案更加完善。CSC 成立于 1899 年，总部位于美国特拉华州威尔明顿市，在美国、加拿大、欧洲和亚太地区设有办事处。CSC 是一家全球性公司，我们通过聘用所服务行业的业内专家，可为世界各地的客户提供服务。欢迎访问 cscdbs.com/cn。

版权所有 ©2026 Corporation Service Company. 保留所有权利。

DBS02132026