解读谷歌新规：所有类型 SSL 证书都必须支持证书自动化

2026 年 6 月 1 日

一、DV SSL 证书自动化已基本普及，但 OV/EV 证书自动化仍处边缘

Let's Encrypt 已占全球 SSL 证书市场的绝对主导地位(近 50%)，发行了超过 10 亿张有效 SSL 证书，每日签发量超千万张。在整个 SSL 证书生态中，DV SSL 证书占比超过 95%，这得益于 ACME（自动化证书管理环境）协议的广泛应用，让域名验证和证书申请完全实现了无人值守的自动化，这意味着国际市场已经基本普及了 DV SSL 证书自动化。

然而，这一繁荣背后隐藏着一个巨大的市场接受度的反差：CA 机构通过几十年的努力说服以后接受 OV 证书，但 OV/EV 证书的自动化签发却几乎没有进展，因为传统观点长期认为，OV 和 EV 证书需要人工完成组织身份验证，因此“不适合”自动化签发流程。

这一认知在国际上已开始被突破，国际头部 CA 已推出面向 OV 和 EV 证书的 ACME 自动化方案，通过“一次人工身份审核、后续全自动化”的模式，用户只需完成一次单位身份的预鉴证，后续的 OV/EV 证书申请、更新和吊销均可通过 ACME 协议自动完成。这表明，OV/EV 证书的自动化在技术上完全没有问题，真正的障碍在于 CA 是否愿意投入改造其证书签发系统。

二、谷歌 V1.8 政策：不向 CCADB 证明自动化能力，就淘汰这个 CA

作为证书自动化的主要推动方—谷歌也认识到这个市场反差问题，于 2026 年 2 月 5 日发布了谷歌浏览器根认证计划 V1.8 版本。其中最关键的一条要求是：**从 2027 年 3 月 15 日起，如果某个 PKI 层级签发的新证书中包含任何基线要求证书政策 OID**（即 2.23.140.1.x 系列，涵盖 DV、OV、IV 和 EV 全部四种证书类型），**但该层级在 CCADB 中缺乏自动化解决方案的证明披露，谷歌浏览器就将启动 CA 淘汰程序。**请注意：2027 年 3 月 15 日同时也是缩短 SSL 证书有效期为 100 天的起始日期。

让我们逐句拆解这条规则的杀伤力。

第一，触发条件是什么？ 任何 CA 下属的任意一个中级根 CA（即一个 PKI 层级），只要

用这个中级根 CA 签发了任意一张包含“基线要求证书政策 OID”的新证书，即无论这张证书是 DV、OV 还是 EV，只要这张证书含有证书类型 OID 的签发行为就自动触发了 CA 向 CCADB 披露自动化能力证明的义务。换句话说，只要 CA 还在签发 TLS/SSL 证书，就必须为签发该证书配备并证明其自动化能力。

第二，什么算“自动化解决方案的证明披露”？ CA 必须为每个类型的 SSL 证书的自动化方案实际运行一个“测试网站”，该网站所呈现的 SSL 证书必须完全由该 CA 根通过自动化方案签发，并且证书必须至少每 30 天自动更新一次。换言之，谷歌要求 CA 用连续不断运行、定期自动更新的“活”证书来证明其自动化能力，而不是在 CCADB 里放一纸空文描述和承诺。请注意：这个自动化更新能力是要求在明年 3 月 15 日之前具备每 30 天更新一次证书的自动化能力，而不是国际标准要求的 2029 年 3 月 15 日起的 47 天有效期，证书可以是 100 天的，但必须每 30 天自动更新一次。

第三，如何证明自动化方案“真实有效”？ CA 必须为每个披露的自动化方案实际运行一个“测试网站”，该网站所呈现的 SSL 证书必须完全由该自动化方案签发，并且证书必须至少每 **30** 天自动更新一次。换言之，谷歌要求 CA 用连续不断运行、定期自动更新的“活”证书来证明自动化能力，而不是在 CCADB 里放一纸空文描述和承诺。**请注意**：这个自动化更新能力是要求在明年 3 月 15 日之前具备每 30 天更新一次证书的自动化能力，而不是国际标准要求的 2029 年 3 月 15 日起的 47 天有效期。

第四，不披露或者披露后被发现造假，后果是什么？ 政策原文写得非常清楚：一旦谷歌检测到违规，例如发现某个中级根 CA 签发了新的证书，但其对应的 PKI 层级在 CCADB 中根本没有自动化方案证明；或者即使有提交自动化证明，但是用于证明自动化能力的测试网站并没有做到每 30 天更新一次证书，谷歌就会为该中级根 CA 设定一个淘汰日期（phase-out date），这个日期定在**违规检测后的 90 天**。90 天之后，谷歌浏览器将不再信任这个中级根 CA 签发的任何新证书，甚至在更新根证书库时直接将根 CA 移出信任列表。

第五，这条规则给了 CA 多长时间缓冲？ 政策自 2026 年 2 月 5 日发布，但实际执行起始日为 2027 年 3 月 15 日。也就是说，全球所有 CA 还有大约 13 个月的时间去改造自己的证书签发系统、建立自动化的 DV/OV/EV 证书签发流程，并在 CCADB 中完成披露，但到今天就只剩下 9 个月了。对于已经具备自动化能力的 CA，这只是一项合规披露工作；但对于那些至今仍然完全依赖人工手动签发 DV/OV/EV 证书的 CA，这意味着必须在一年之内完成从“人工模式”到“自动化模式”的彻底转型，否则其 SSL 证书业务将在 2027 年 3 月 15 日之后被谷歌浏览器直接掐断。对于已经具备自动化基础的 CA，这只是一项合规披露工作；但对于那些至今仍然完全依赖人工手动签发 DV/OV/EV 证书的 CA，这意味着必须在一年之内完成从“人工模

式”到“自动化模式”的彻底转型，否则其 SSL 证书业务将在 2027 年之后被谷歌浏览器直接掐断。

第六，政策背后的深层逻辑是什么？ 很多人误以为谷歌只是“建议”CA 拥抱自动化，或者认为 OV/EV 证书因为涉及身份验证可以豁免。但 V1.8 版本彻底打破了这一幻想：政策明确将 OV 和 EV 证书的 OID（2.23.140.1.2.2 和 2.23.140.1.1）列入了必须提供自动化证明的范围，没有任何例外。谷歌之所以如此强势推进，根源在于 CA/浏览器论坛的基线 BR 要求早已为自动化扫清了技术障碍。首先，BR 的 3.2.2.4 节明确规定，CA 在验证企业身份时可以采用“可靠的外部数据源”，例如政府数据库、征信机构等，并不必然依赖人工线下核查，这意味着 OV 和 EV 证书的身份验证环节完全可以被标准化、自动化地完成。其次，IETF 早在 2019 年就发布了 RFC 8555（即 ACME 协议），BR 也早已将其采纳为行业标准，为证书的自动化申请、域名验证和吊销提供了完整的技术框架。谷歌此次强制要求 CA 在 CCADB 中披露其自动化方案，本质上就是将 BR 已经允许的“自动化验证”和已经采纳的“ACME 标准”从“可选项”升级为“**必选项**”。因此，谷歌强制要求所有类型 SSL 证书全部支持自动化，既是对 BR 既有精神的落地，也是为证书有效期不断缩短政策的落地铺路，也是回应了用户对 OV 证书的自动化需求。

总而言之，谷歌 V1.8 政策不是一份建议书，而是一张带有明确时间表和执行机制的“**最后通牒**”。它向全球 CA 发出了一个清晰无误的信号：**要么让你的 OV/EV 证书也能像 DV SSL 证书一样全自动签发，要么你就放弃签发 OV/EV SSL 证书，或者放弃谷歌浏览器信任。**

三、我国国密 SSL 证书自动化正面临前所未有的机会窗口

谷歌的这一政策调整，看似面向国际 PKI 体系，实际上为我国的国密 SSL 证书自动化提供了绝佳的加速动力。原因很简单：如果国际市场要求 OV/EV 证书也必须支持自动化签发，那么中国 CA 在改造国际 SSL 证书签发系统的同时，完全可以将同样的自动化能力复用于国密 SSL 证书。

但目前我国国密 SSL 证书的自动化现状并不乐观。绝大多数 CA 至今仍然签发一年有效期的国密 SSL 证书，仅有极少数 CA 实现了国密 SSL 证书的自动化签发。这种现状与已经生效的证书有效期不断缩短形成了尖锐的矛盾。如果国密 CA 依然依赖一年一签的人工手动模式，届时将根本无法应对平均每月一次的证书更新需求。

零信技术早在 2023 年就已发布的国密 HTTPS 加密自动化网关，正是这一趋势的前沿实践。该自动化网关默认配置为“国密 OV+国际 DV”双证书模式，实现了国密 OV SSL 证书的自动化申请、云 SSL 服务系统的自动化身份验证和域名验证以及自动化签发、自动化网关的自

动化部署。这证明了自动化签发国密 OV SSL 证书不仅在技术上完全可行，而且已经是一个可商用的成熟方案。

零信浏览器的实践同样具有示范意义。零信浏览器已修订了国密 SSL 证书有效期的验证规则，同步谷歌浏览器一样不信任超过国际标准规定有效期的国密 SSL 证书，与国际标准保持一致。这一举措传递了一个明确的信号：证书有效期缩短是大势所趋，唯有自动化才是未来。

谷歌新规给我们带来的最重要启示是：所有类型 SSL 证书的自动化签发不是“可选项”，而是浏览器信任的“**必选项**”。建议我国 CA 应当抓住这个窗口期，借国际 SSL 证书自动化的经验，加快国密 SSL 证书自动化服务能力的改造，采用自动化方式快速普及国密 SSL 证书应用。零信技术的国密 OV+国际 DV 双证书自动化的成功实践已经证明，这条路不仅走得通，而且走得很好，同时满足了用户对国密 OV 证书和证书自动化管理的迫切需求。

王高华

2026 年 6 月 1 日于深圳

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。
已累计发表中文 274 篇(共 81 万 3 千多字)和英文 119 篇(16 万 6 千多单词)。