# 解读 Sectigo 2024 年预测一：拥抱浪潮—证书自动化将颠覆各个行业

零信技术国际 SSL 证书战略合作伙伴 Sectigo 本月在其官网博客栏目发布了 2024 年数字安全领域的五大预测，笔者利用周末时间翻译并解读了这五大预测。

今天解读预测一：自动化将改变所有行业。

自动化始于工业革命时期，实现了自动化流水线生产，采用大量的机器来替代人工而降低成本和减少差错。自动化从制造业到服务业，已经渗透到社会生活的方方面面，包括当下的人工智能实现的各种自动化。本预测所讲的重点是 SSL 证书的自动化部署和自动化实现 HTTPS 加密，这是因为实现 HTTPS 加密是所有行业实现自动化的核心应用，是实现自动化所需的数据流通安全的根本保障，所以，笔者把原英文标题直接翻译为：证书自动化将颠覆各个行业，下面就详细解读这个观点，将有助于读者能读懂后面的 Sectigo 博文的中文译文。

对于 CA 机构，如果还停留在销售 SSL 证书的阶段，是一定会被淘汰的，因为全球 6.5 亿张有效 SSL 证书中超过 80%都是自动化申请和部署的，用户需要的是 HTTPS 加密服务，而不是 SSL 证书，只有帮助用户自动化实现 HTTPS 加密才是正道。而引领证书自动化的是软件厂商和云服务提供商，全球 SSL 证书市场份额排名的前 4 名都不是传统的 CA 机构，这就印证了一个至理名言--真正打败你的往往不是你的同行，他们成功的秘诀就是自动化，所以 CA 机构必须及时积极拥抱证书自动化。而普及应用商密 SSL 证书，则更需要自动化解决方案，帮助用户零改造实现商密 HTTPS 加密。

对于云服务提供商，如果还停留在云主机的价格战中，则一定是满盘皆输。在 HTTPS 加密无处不在的当代，在数据大流通的时代，必须把 HTTPS 加密自动化服务紧密集成到各种云产品和云服务，才能增强其核心竞争力，才能赢得云服务市场。这也是国际上云服务大厂如谷歌、Cloudflare、亚马逊、微软等赢得云市场的秘诀，而且同时成功跨界成为 SSL 证书市场的领先者。

对于各省市政务云平台，要管理成千上万个网站和业务系统的 HTTPS 加密应用，人工申请和部署 SSL 证书绝对是一件无法实现的目标，也就根本不可能实现采用商用密码来保障关键信息基础设施的安全的目标和合规要求。唯一的解决方案是自动化证书管理，零改造完成国密 HTTPS 改造，把需要人工处理的工作交给机器去做，这个机器就是国密 HTTPS 加密自动化网关，自动化申请和部署双算法 SSL 证书，自动化实现自适应加密算法的 HTTPS 加密。自动化是政务云平台完成商密改造的唯一解决方案，不是之一而是唯一。

对于智慧城市建设，目前大量的数据采集和数据处理过程都是 HTTP 明文传输，不仅使得这些重要数据在传输过程中非常容易被非法窃取，做成大量敏感数据泄密，而且使得这些重要数据在传输过程中非常容易被非法篡改，导致采集的数据严重失真，甚至错误的数据导致人工智能算法得出错误的结果而造成巨大的损失和带来巨大的安全风险。所以，所有智慧城市系统都需要拥抱自动化证书管理，零改造实现数据采集通道的自动化 HTTPS 加密传输，从而保障各种数据的传输和流通安全。这对于车联网和物联网也是一样的重要。

对于工业互联网安全，目前也是大量的工业设备数据采集和设备控制都是 HTTP 明文传输，这严重威胁了工业互联网的数据传输安全，也就是威胁了工业生产安全。一样也只有全部实现证书自动化，自动化实现工业数据传输的 HTTPS 加密，才能保障工业数据的采集和设备控制的安全，保障工业互联网安全，从而保障工业生产自动化安全。

数字化转型的关键是万物互联，数据的价值在于流通，互联和流通的安全的关键是 HTTPS 加密，在我国则是商密 HTTPS 加密。而要实现 HTTPS 加密，也只有自动化一条路，传统的手动申请和部署证书方式在 HTTPS 泛在的应用场景下变成了不可能。

所以，正如 Sectigo 预测所讲，一切自动化的核心是证书自动化，自动化实现 HTTPS 加密，才能保障其他自动化革命的成功和健康蓬勃发展。拥抱证书自动化浪潮就是勇立潮头，抓住了自动化的核心，将在一个以无缝自动化服务为特征的新时代获得并保持核心竞争力。

**<下面请读者朋友仔细阅读原文译文>**

证书自动化有望标志着另一个重要的里程碑—转变和重新定义各种规模的企业和行业。自动化的激增将促进已经互联的数字基础设施的发展。我们将看到一个无缝自动化服务的世界。


随着新年的临近，2024 年将是一个变革时期，尤其是在自动化领域。 自动化不仅重新定义了企业级运营，而且将渗透到各种规模的企业和行业。这场革命的关键参与者是证书自动化，

预计它将在明年达到峰值里程碑。

证书自动化曾经局限于大型企业的领域，现在正在突破以前的界限，在所有企业和行业中留下不可磨灭的印记。自动化浪潮的连锁反应有望将已经互联的数字基础设施错综复杂地编织在一起，预示着一个以无缝自动化服务为特征的新时代的到来。

## 技术的演变

这一浪潮背后的驱动力在于技术的不断演进。 随着人工智能、机器学习和数据分析的进步，自动化变得更加复杂和适应性更强。 因此，企业越来越认识到需要将自动化集成到其运营中，以在动态的技术和网络安全环境中保持竞争力。

也许自动化的定义特征是它能够简化流程和提高效率。证书自动化发挥着关键作用，不仅可以降低总体拥有成本，还可以强制执行加密合规性并防止人为错误造成的潜在服务中断。传统上，证书自动化只管理 SSL 证书，但证书自动化现在已经涵盖更广泛的任务。 从身份验证流程到加密密钥管理，证书自动化正在成为确保数字交易完整性和安全性的基石。

## 互联互通的数字环境

自动化的影响不仅仅是运营效率，它正在重塑商业架构。随着自动化变得更加容易获得和必不可少，大型企业和小型企业之间曾经清晰的界限正在逐渐消失。数字证书的寿命正在缩短，对于首席信息安全官(CISO)及其团队来说，这代表着他们未来建立数字信任的方式将发生了重大变化。通过使用电子表格和孤立的单点解决方案进行证书生命周期管理的手动或传统证书管理方法已不再可行。

数字基础设施的互联性是这场自动化革命的关键推动力。自动化在数据无缝流通于各种系统之间的环境中蓬勃发展，到 2024 年，我们可以期待一个更加互联的环境。这不仅将促进信息交换，还将为更加协作和集成的业务运营方法奠定基础。

## 现在就着手实现证书自动化

2024 年将是自动化的标志性一年，证书自动化将成为重塑行业的中心舞台。这种激增的影响不仅仅是技术进步，而且它标志着企业(无论规模大小)在数字时代的运营和竞争方式发生了根本性转变。随着我们拥抱自动化浪潮，我们正在迎来一个效率、安全和协作三融合的时代，重新定义企业的未来。

王高华

2023 年 12 月 18 日于深圳

---

请关注公司公众号，实时推送公司 CEO 精彩博文。