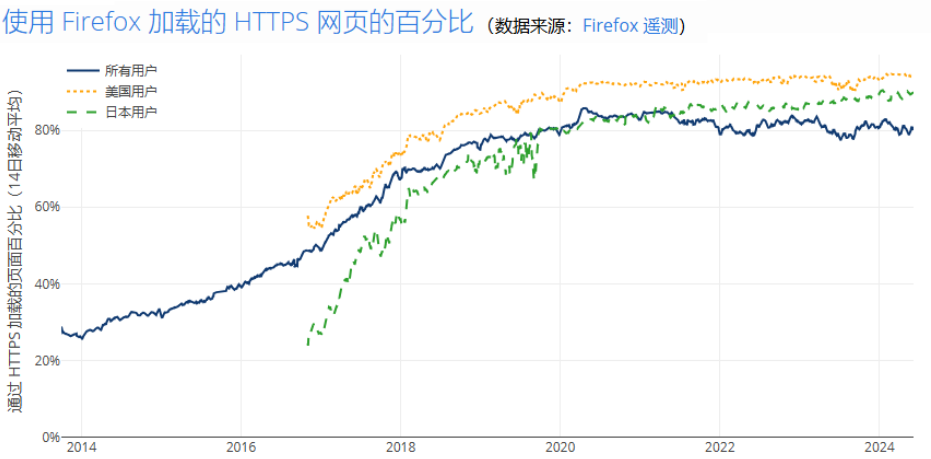
SSL 证书自动化是普及实现 HTTPS 安全连接的唯一方案

四部委联合发布的《互联网政务应用安全管理规定》七月一日正式施行，倒计时 20 天。相信相关单位 IT 主管们都在想办法如何能满足规定的要求，这个事情一定不是向 CA 申请一张 SSL 证书那么简单的事情。笔者最近参加了多个会议和同多个合作伙伴交流，深深感到用户和密码从业者并没有真正认识到 SSL 证书自动化的伟大意义。结合《规定》的紧迫性，笔者特撰写本文，帮助广大用户，特别是正在寻找解决方案的政府单位用户，以及密码从业者，都能准确理解 SSL 证书自动化这个改变世界的技术创新的伟大之处，理解了这个，就能找到正确的快速实现 HTTPS 加密的解决方案。希望本文能帮助大家更深刻地认识 SSL 证书自动化的重要性、必要性和紧迫性。

一、什么是 SSL 证书自动化？为何说这是改变世界的技术创新？

SSL 证书是实现 HTTPS 加密必须的密码产品，传统方式是用户向 CA 人工申请 SSL 证书，人工部署到 Web 服务器上实现 HTTPS 加密，这个过程非常繁琐，熟练工程师最少也需要两个小时才能完成 DV SSL 证书申请和部署工作，如果是申请 OV/EV SSL 证书则需要等 1-3 天。这就使得 HTTPS 加密普及应用受到了极大的制约，从 1994 年 Netscape 发明了 SSL 证书，到 2014 年 20 年时间全球实现了 25%网站的 HTTPS 加密。

而从 Let’s Encrypt 免费 SSL 证书自动化项目 2013 年问世(一个软件厂商的杰作)，到现在 10 年时间就实现了全球 80%以上的网站的 HTTPS 加密，这个普及 HTTPS 加密的加速度的实现当然必须归功于 SSL 证书的自动化签发和自动化部署。



从 2013 年有统计数据起，全球 CA 已经累计签发了全球信任的 RSA/ECC 算法 SSL 证书超过 160 亿张，截止到今天，有效 SSL 证书有 7.36 亿张，而这 7.36 亿张证书有 3.77 亿张 SSL 证书由 Let’s Encrypt 签发，超过 50%市场份额，全球排名第一，单日证书签发量高达 5 万多张，这就是自动化的威力和魅力。

Let’s Encrypt 不仅自己实现了自动化签发 RSA/ECC 算法 SSL 证书，而且牵头制定了国际标准 RFC 8555 (ACME，自动化证书管理环境)，从而带动了整个业界都开始实现 SSL 证书自动化签发管理，使得互联网公司和云服务提供商有机会弯道超车，一举超过老牌 CA 机构，排名第二位的是互联网公司(域名注册商)-GoDaddy、排名第 3 位的是云服务提供商-亚马逊、排名第 4 位的是互联网巨头-谷歌、原先排名第一个第二的传统 CA 机构 DigiCert 和 Sectigo 排到了第 5 位和第 6 位，微软排名第 7 位，CDN 服务提供商 Cloudflare 排名第 8 位。这就是自动化给这些互联网大厂的机会，因为他们手中有用户，而用户则需要一站式自动化解决方案。希望国内互联网公司和云服务提供商能从中看到商机，也希望国内 CA 机构能从中看到危机。

传统的 SSL 证书申请和部署，最快也要花费一个工程师两个小时的时间，如果现在的全球 7.36 亿张 SSL 证书仍然是工程师人工手动申请和部署的话，则将费时 15 亿小时，如果一个工程师安装，则需要近 2 亿天才能完成。如果希望 2 小时完成的话，则需要 1.8 亿个工程师，这些都是人工无法完成的天文数字，但是自动化让这些数字成为现实，这就是自动化的威力。对于单位决策者来讲，申请和安装 SSL 证书这些繁琐的费力的工作完全可以由机器来自动化实现，为何还要浪费宝贵的工程师去做这些呢？自动化在各行各业的成功已经证明了自动化的威力，这是必选之路。

同理，SSL 证书普及应用之路也是自动化，自动化申请和部署为普及应用 HTTPS 加密立了大功，大大提升了全球互联网应用的安全，特别万物互联的安全，这就是一个改变世界的技术创新，是一个很重要的密码应用创新。没有这个技术创新，现在全球 SSL 证书应用仍然徘徊在 25%的使用水平上，大量的数据处于裸奔状态，那就不可能有现在的移动互联网、车辆网、物联网等万物互联的繁荣和飞速发展。

也正是由于全球 90%以上的 SSL 证书实现了自动化，所以，为了 SSL 证书密钥安全，谷歌于去年 3 月份发起了推动 SSL 证书有效期缩短为 90 天的计划，意在提高将整个生态系统快速过渡到抗量子算法所需的敏捷性，这也是 SSL 证书自动化带来的可能性，密钥的更新速度提升将大大提升 HTTPS 加密的安全性能。笔者预计 90 天 SSL 证书有效期的政策会在今年年底落地，到了那个时候，现在的每年一次的人工申请证书和安装 SSL 证书的传统方式将不

复存在，这个发展趋势非常值得用户和业界高度重视，必须提前做好心理准备和技术准备，否则到时措手不及而导致大量的业务系统由于 SSL 证书无法正常续期而中断服务。

二、为何商密 HTTPS 加密更需要自动化？

同全球市场不同的是，我国的 SSL 证书自动化应用非常落后，几乎 100%的 SSL 证书仍然停留在传统的人工申请和部署 SSL 证书阶段，这是导致我国网站的 SSL 证书的普及率低于 20%的主要原因。下图是 2024 年 Q1 的各省政务网站申请 SSL 证书的统计数据，一个省有超过一万个互联网政务网站，但是 SSL 证书申请量最多只有 216 张，最少只有 31 张，说明还要大量的网站没有部署 SSL 证书。为什么？因为人工申请和部署 SSL 证书太难了，这是 RSA 算法 SSL 证书的情况。而实现商密 HTTPS 加密就更难了，不仅需要申请和部署商密 SSL 证书，还要改造 Web 服务器来支持商密算法，这就难怪 31 个省市自治区政府官网只有一个湖南省官网实现商密 HTTPS 加密。

排名	省市自治区	数量	增长%	占比%	检索域名	默认https	部署国密
1	上海市	216	10.77%	13.23%	shanghai.gov.cn, sh.gov.cn	是	否
2	浙江省	189	-5.03%	11.57%	zj.gov.cn	是	否
3	北京市	130	-0.76%	7.96%	beijing.gov.cn	是	否
4	海南省	107	5.94%	6.55%	hainan.gov.cn	是	否
5	广西壮族自治区	96	5.49%	5.88%	gxzf.gov.cn	否	否
6	广东省	76	0.00%	4.65%	gd.gov.cn	否	否
7	云南省	65	16.07%	3.98%	yn.gov.cn	是	否
8	天津市	62	1.64%	3.80%	tj.gov.cn	是	否
9	宁夏回族自治区	62	-1.59%	3.80%	nx.gov.cn	是	否
10	河南省	56	7.69%	3.43%	henan.gov.cn	是	否
11	山东省	49	-2.00%	3.00%	shandong.gov.cn, sd.gov.cn	否	否
12	江西省	45	4.65%	2.76%	jiangxi.gov.cn	否	否
13	陕西省	42	7.69%	2.57%	shaanxi.gov.cn	否	否
14	甘肃省	41	5.13%	2.51%	gansu.gov.cn	是	否
15	吉林省	40	-4.76%	2.45%	jl.gov.cn	否	否
16	安徽省	38	8.57%	2.33%	ah.gov.cn	是	否
17	贵州省	36	5.88%	2.20%	guizhou.gov.cn	否	否
18	黑龙江省	35	133.33%	2.14%	hlj.gov.cn	是	否
19	新疆维吾尔自治区	33	50.00%	2.02%	xinjiang.gov.cn	是	有(登录页)
20	重庆市	33	-5.71%	2.02%	cq.gov.cn	是	否
21	湖南省	32	-11.11%	1.96%	hunan.gov.cn	否	有
22	河北省	31	34.78%	1.90%	hebei.gov.cn	否	否
23	福建省	20	-20.00%	1.22%	fujian.gov.cn, fj.gov.cn	是	否
24	江苏省	19	18.75%	1.16%	jiangsu.gov.cn, js.gov.cn	否	否
25	青海省	16	0.00%	0.98%	qinghai.gov.cn	否	否
26	内蒙古自治区	15	15.38%	0.92%	nmg.gov.cn	是	否
27	辽宁省	14	0.00%	0.86%	ln.gov.cn	是	否
28	西藏自治区	12	9.09%	0.73%	xizang.gov.cn	否	否
29	山西省	11	0.00%	0.67%	shanxi.gov.cn	是	否
30	湖北省	8	14.29%	0.49%	hubei.gov.cn	否	否
31	四川省	4	0.00%	0.24%	sc.gov.cn	是	否
	合计	1633	5.02%			18	2

以上数据是 RSA 算法 SSL 证书的部署情况，而为了保障我国互联网政务应用安全，根据《规定》第二十九条要求，HTTPS 加密必须采用电子政务电子认证服务机构签发的商密 SSL 证书来实现商密 HTTPS 加密。这个规定对于机关事业单位和列入关键信息基础设施的运营单位来讲，可以说是一个必须尽快找到解决方案的大事，因为第四十一条规定“对违反或者未能正确履行本规定相关要求的，按照《党委（党组）网络安全工作责任制实施办法》等文件，依规依纪追究当事人和有关领导的责任。”而传统的人工申请 SSL 证书和部署 SSL 证书根本无法完成这个艰巨的任务，怎么办？

答案是自动化，只有证书自动化这一条路可走，大家从第一部分就已经看到自动化的魅力和威力。但是，国际上采用的自动化解决方案仅适用于 RSA 算法 SSL 证书，对于机关事业单位来讲，必须实现商密 SSL 证书的自动化，否则无法实现所有互联网政务应用的大规模部署应用。

但是，商密 SSL 证书自动化无法复制国际 SSL 证书自动化的解决方案，因为仅有商密 SSL 证书无法实现商密 HTTPS 加密，需要整个生态产品和系统都支持商密算法，包括但不限于浏览器、Web 服务器、CA 系统、操作系统、CDN 服务、WAF 设备或云 WAF 服务等等，这就需要商密改造。但是，改造一个已经渗透到每一个应用角落的 RSA 密码体系谈何容易！只有一个字：难！两个字：很难！

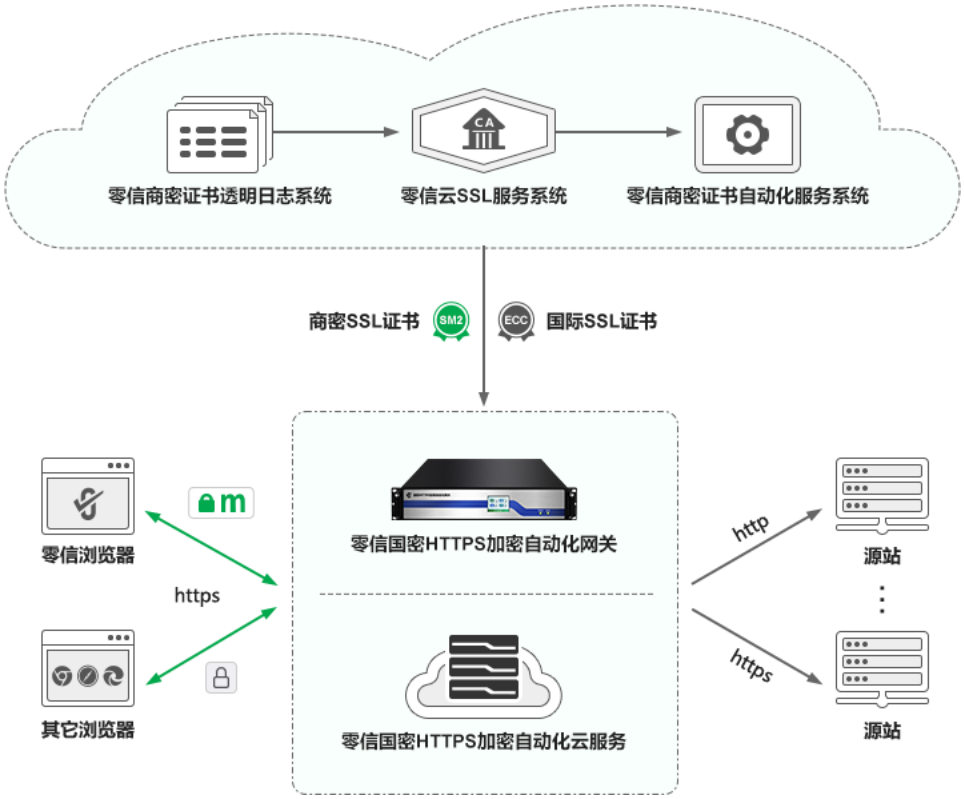
三、零信技术在商密 SSL 证书自动化方面做了哪些创新工作？

商密改造很难，但这事必须做，并且必须尽快完成！《规定》7 月 1 日施行！怎么办？

零信技术早在 3 年前就创新地提出了一个零改造的解决方案，很难改造，那就不改造！原系统不动，直接在原系统前面加一个 HTTPS 加密自动化网关来实现商密 HTTPS 加密，一个自动化配置 SSL 证书自动化实现 HTTPS 加密的网关—零信国密 HTTPS 加密自动化网关彻底解决商密改造难题。

零信技术历时 3 年彻底解决了商密 SSL 证书自动化难题，创新地打造了商密证书透明和商密证书自动化管理两个商密应用生态。这是一个端云一体实现商密 SSL 证书自动化管理的创新解决方案，原 Web 服务器零改造的自动化完成商密 HTTPS 加密改造，让商密改造不再难，可以快速实现商密 HTTPS 加密自动化。更加难得的是，零信技术 SSL 证书自动化管理解决方案是商密 SSL 证书和国际 SSL 证书双证书自动化解决方案，自动化为用户网站配置双 SSL 证书，以满足用户的商密合规和全球信任的双需求，因为互联网服务不能也无法强制要

求用户使用何种浏览器，必须支持所有浏览器，无论这个浏览器是否支持商密算法和商密 SSL 证书。



零信商密 SSL 证书自动化管理解决方案的核心产品是零信国密 HTTPS 加密自动化网关(简称“零信网关”)，这是我国首个通过商密产品认证商密 HTTPS 加密自动化网关，用户网站服务器无需任何改造，直接在前面部署零信网关即可，由零信网关自动对接零信云 SSL 证书为用户网站自动化签发商密 SSL 证书和国际 SSL 证书，双 SSL 证书自动化部署，自动化实现 HTTPS 加密，支持商密算法的商密浏览器优先采用商密算法实现商密 HTTPS 加密，不支持商密算法的其他浏览器则采用 RSA 算法实现 HTTPS 加密，从而自动化满足《规定》所要求的实现使用安全连接方式访问互联网政务应用的要求。同时，零信网关内置 WAF 防护功能模块，自动化为用户提供 HTTPS 加密和 Web 应用安全防护，双重保障用户网站安全。而对于无法部署或不想部署硬件网关的用户，则可以共享使用部署在云上的零信网关为网站提供商密 HTTPS 加密自动化云服务，一样可以自动化实现 HTTPS 加密和 WAF 防护。

零信商密 SSL 证书自动化管理解决方案的另一个核心产品是零信浏览器，这是目前市场上唯一一个完全免费的、干净无广告的、支持商密证书透明的、基于谷歌 Chromium 114 内核的商密浏览器，因为商密 HTTPS 安全连接访问必须要有浏览器支持，普及商密 HTTPS 加密需要有完全免费的商密浏览器。

零信浏览器与零信网关紧密配合，只采用商密算法实现 HTTPS 加密和 WAF 防护，不怕 RSA 算法 SSL 证书被吊销和被断供，完全用商密算法来保障我国网站的机密信息传输安全，有力保障我国大数据流通安全，保障我国各行各业的数字化转型安全。

SSL 证书自动化是必由之路，也是一个改变世界的创新解决方案，使得全球在短短的十年实现了 HTTPS 加密的 80%的覆盖率。我国要想普及商密 SSL 证书实现 HTTPS 加密，也只有自动化这一条路，这是解决目前互联网政务应用急需普及应用商密 HTTPS 加密的唯一可行解决方案。

零信商密 SSL 证书自动化管理解决方案，2023 年 11 月在第二十五届中国国际高新技术成果交易会首发并荣获组委会颁发的优秀产品奖证书，同时这个解决方案也得到了国家密码行业标准化技术委员会的认可，于 2023 年 12 月批准由零信技术牵头制定《自动化证书管理规范》和《证书透明规范》两个商密标准，意在引领业界依据商密标准来共同实现商密 SSL 证书的自动化管理，并且实现自动化签发的商密 SSL 证书支持证书透明，从而安全可靠地自动化实现商密 HTTPS 加密，快速普及商密 HTTPS 加密来保障我国网络空间安全，包括保障《规定》要求的互联网政务应用安全。

王高华

2024 年 6 月 11 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 168 篇(共 45 万 6 千多字)和英文 68 篇(8 万 4 千多单词)。。