

## 中国 SSL 证书市场发展趋势分析简报-2023Q4

2024 年 1 月 2 日

本报告由零信技术**零信任安全研究院**全球独家发布，电子版首发渠道为零信任安全研究院微信公众号：zotrusi 和零信官网 CEO 博客栏目(HTML 版本和 PDF 版本(有数字签名和时间戳))。

本次发布的是定期发布的 2023 年第四季度分析报告，希望对我国 SSL 证书的产业发展和普及应用起到积极推动作用，特别是国密 SSL 证书的普及应用。本次简报继续发布全球 CA 为我国政府域名\*.gov.cn 签发的 SSL 证书的数据，这个重要领域的 SSL 证书签发数据非常有参考价值，可用于有关部门研判风险和制定相关风险管理政策。本次发布的报告由于是年末发布，所以特增加一个年度总结段落，希望这些数据和建议能为相关部门和机构的相关决策提供有力参考。

### 一、全球 SSL 证书统计数据分析

根据国际证书透明日志系统数据统计，截止到 **2023 年 12 月 30 日**，已经在国际证书透明日志系统记录的全球 SSL 证书总数已经达到 **116 亿**多张，其中未过期的全球信任的 SSL 证书有 **6.7644 亿**张，比上一季度增加了 **10.10%**。

全球 **6.7644 亿**张有效证书中，只验证域名的 DV SSL 证书有 **5.7848 亿**张，比第一季度增加了 **12.45%**，占比 **85.52%**，增加了 1.78 个百分点，意味着 DV SSL 证书的比例在持续增长。验证网站身份的 OV SSL 证书有 9759 万张，扩展验证网站身份的 EV SSL 证书 **34.297 万**张，占比 **0.05%**。鉴于 Cloudflare 自动化签发了大量的 O 字段为 Cloudflare 的 OV SSL 证书，但实际上是为使用 Cloudflare CDN 服务的网站签发的，数量为 5071 万张，这些 OV SSL 证书可以理解为是错误签发的 OV SSL 证书，实际上是 DV SSL 证书！也就是说，OV SSL 证书实际数量少于 4688 万张，占比仅为 **6.93%**。所以，实际上，DV SSL 证书占比为 **93.02%**，这是一个非常有意义的数字，意味着 DV SSL 证书已经一统天下，非 DV SSL 证书仅占不到 **7%**！

全球 **6.1436 亿**张有效证书中，排名前十大 SSL 证书提供商分别是：第 1 位仍然是 Let's Encrypt (3.1085 亿张)(比上一季度增加了 6.34%，首次超过了 50%市场份额)、第 2 位是谷歌(5736 万张)(上升了 1 位)(增加)、第 3 位是亚马逊(5441 万张)(上升了 1 位)(增加)、第 4 位是 Cloudflare (5071 万张)(下降了 2 位)(减少)、第 5 位是 GoDaddy(4844 万张)(上升了 2 位)(增加)、第 6 位是 Sectigo (4399 万张)(下降了 1 位)(增加)、第 7 位是 DigiCert (3307 万张)(下降了 1 位)(增加)、第 8 位是 ZeroSSL (2490 万张)(上升了 1 位)(增加)、第 9 位是微软 (2242 万张)(下降了 1 位)(减少)、第 10 位是 cPanel(1227 万张)(减少)。对比上一季度的数据，谷歌跃到了第二位，实现了在 2016 年启用自己的根证书时确定的目标。互联网公司 GoDaddy 上个季度增加了 216%，从 9 位上升到第 7 位，这个季度比上个季度增加了 188%，势头很猛，这个数据不知道是否对我国互联网公司和云平台公司能有所启发，GoDaddy 由注册域名起家，拥有大量域名用户，就可以把建站用的 SSL 证书市场也一并拿下，绝招仍然是自动化为用户实现 HTTPS 加密。两个季度连续下跌最多的仍然是 cPanel，意味着虚拟主机用户已经开始转向云服务提供商，其产品已失去了核心竞争力。

全球排名前十的 SSL 证书提供商中，传统的 CA 机构 Sectigo 和 DigiCert 没有保住其第 5 和第 6 位，都下降了一位，这也是预料之中的事情，因为互联网公司和云平台服务商都已经为用户自动化提供 SSL 证书和自动化实现 HTTPS 加密了，还有用户会去费力向 CA 申请 SSL 证书再去费力安装吗？这是 CA 的劣势，而如何突破这个劣势，唯一的突破口仍然是自动化，一个同互联网公司和云平台商不一样的自动化，而不是学习他们的自动化方案，因为最终用户在他们手中，如果你的解决方案同他们一样，用户怎么会去用你的方案呢？这一点值得所有 CA 机构反思。

本季度的数据中的 DV SSL 证书比例已经高达 93%，这个数据非常值得重视，因为谷歌在 3 月 3 日发布了将来的计划，将推动国际标准缩短 SSL 证书有效期为 90 天。谷歌发布这个计划是有底气，因为目前全球

有效 SSL 证书中已经有 93%都是 90 天有效期的证书，虽然这个比例在我国并没有这么高，但是这个数据非常值得重视。唯一的出路大家应该已经看到了，只有自动化实现 SSL 证书的申请、部署和续期，这是唯一的一条路，不仅国际 SSL 证书如此，国密 SSL 证书也是如此。

## 二、我国政府网站的 SSL 证书统计数据分

我国已经基本上实现了所有政务服务“一网通办”的目标，但是政府网站和电子政务系统的安全状况如何，可以从 SSL 证书的申请量来反映。我国各省市已经启动了全省一个主域名，下属各局委办都是使用其子域名的管理方式，所以，我们检索了一个省的主域名就能得到这个省的省级政府网站一共申请了多少张 SSL 证书，如广东省统计\*.gd.gov.cn 的域名(这里的\*指 gd.gov.cn 下的所有子域名)，各地市使用了自己域名，如深圳市的\*.sz.gov.cn 并不在广东省的统计数据中。如果某省市启用了两个域名，如上海市的 sh.gov.cn 和 shanghai.gov.cn，则合并统计两个域名的 SSL 证书申请数量。

具体数据如下表 1 所示，31 个省市自治区省级政府域名所申请的有效 SSL 证书数量合计为 1555 张，比上一季度增加了 8.36%。其中，海南省又上升了一位，升到第 4 名，可能与海南封关有关，必须抓快与国际接轨，所有政务网站都需要有 HTTPS 加密。山东省上升了 5 位，其他排名上升还有新疆自治区、湖南省等，排名前 5 位的是浙江省、上海市、北京市、海南省、广西壮族自治区。

排名	省市自治区	数量	增长%	检索域名	默认https	部署国密	WAF防护	安全评级
1	浙江省	199	-4.78%	zj.gov.cn	是	否		B+
2	上海市	195	11.43%	shanghai.gov.cn, sh.gov.cn	是	否		B
3	北京市	131	13.91%	beijing.gov.cn	是	否	有	B+
4	海南省	101	23.17%	hainan.gov.cn	是	否		B+
5	广西壮族自治区	91	-1.09%	gxzf.gov.cn		否		
6	广东省	76	4.11%	gd.gov.cn		否		
7	宁夏回族自治区	63	0.00%	nx.gov.cn	是	否		B+
8	天津市	61	7.02%	tj.gov.cn	是	否	有	A
9	河南省	52	15.56%	henan.gov.cn	是	否		B+
10	山东省	50	35.14%	shandong.gov.cn, sd.gov.cn		否		
11	江西省	43	-2.27%	jiangxi.gov.cn		否		
12	吉林省	42	10.53%	jl.gov.cn		否	有	
13	云南省	56	47.37%	yn.gov.cn	是	否		B+
14	陕西省	39	-2.50%	shaanxi.gov.cn		否		
15	甘肃省	39	14.71%	gansu.gov.cn	是	否		B+
16	湖南省	36	33.33%	hunan.gov.cn		否	有	
17	重庆市	35	-16.67%	cq.gov.cn	是	否		
18	安徽省	35	12.90%	ah.gov.cn	是	否	有	A
19	贵州省	34	9.68%	guizhou.gov.cn		否		
20	福建省	25	25.00%	fujian.gov.cn, fj.gov.cn	是	否		B+
21	河北省	23	9.52%	hebei.gov.cn		否		
22	新疆维吾尔自治区	22	69.23%	xinjiang.gov.cn	是	有(登录页)		B
23	青海省	16	-11.11%	qinghai.gov.cn		否		
24	江苏省	16	6.67%	jiangsu.gov.cn, js.gov.cn		否		
25	黑龙江省	15	7.14%	hlj.gov.cn	是	否	有	A
26	辽宁省	14	-6.67%	ln.gov.cn	是	否		B+
27	内蒙古自治区	13	0.00%	nmg.gov.cn	是	否	有	A
28	山西省	11	-15.38%	shanxi.gov.cn	是	否		B+
29	西藏自治区	11	10.00%	xizang.gov.cn		否		
30	湖北省	7	0.00%	hubei.gov.cn		否		
31	四川省	4	33.33%	sc.gov.cn	是	否		B+
	合计	1555	8.36%		18	2	6	

表 1

对于国密算法 SSL 证书的部署情况，本季度无新增，31 个省市自治区省级政府官网中部署了国密 SSL 证书的仍然只有一个湖南省政府门户网站。从这个数据可以看出国密改造之难，唯一可行的解决方案只有部署零改造的国密 HTTPS 加密自动化网关，自动化实现国密 HTTPS 加密，只有这样才能普及实现国密 HTTPS

加密来保障电子政务系统安全。

对于默认 HTTPS 加密这一项，本月只有 17 个省政府官网自动启用 HTTPS 加密，虽然有多个省政府网站已经部署了 SSL 证书，但是并没有自动切换到 HTTPS 加密方式，这等于没有部署 SSL 证书，并没有起到加密保护的作用，因为用户并不会手动加上 https 来访问的。据了解，这是考虑到 HTTPS 加密会增加服务器的加解密负担而故意这样设置的，如果真的是这个原因，推荐在服务器之前部署国密 HTTPS 加密自动化网关，把 HTTPS 加解密任务交由网关来完成，并且不用人工申请和部署 SSL 证书，一箭双雕，这才是最佳解决方案，而不应该担心服务器负载情况而不启用 HTTPS 加密。

对于省政府官网是否有云 WAF 防护这一项，31 个省市自治区中有 6 个省政府网站有 WAF 防护，但是只有 5 个网站同时启用了默认 https 加密，也就是只有这 5 个网站的 WAF 防护才真正发挥防护作用。当然，我们无法知道这些网站是否采用了本地化部署了 WAF 设备防护，所以这项数据仅供参考。本次统计的“安全评级”项的数据来自于零信浏览器的实时评级，对于没有默认启用 https 加密的网站不参与安全评级。

我们检索了 \*.gov.cn 的 SSL 证书申请量为 16917 张，比上一季度增加了 3.90%，这是我国各省市所有政府网站的总量(不包括港澳台地区)，含上面统计数据中的 1555 张。从本期开始，我们将具体列出这些 SSL 证书有多少张 DV/OV/EV SSL 证书、由哪些 CA 签发，各个 CA 的签发数量排名。为何需要分析这些数据，因为只有知道了政府网站 https 加密 SSL 证书是哪些 CA 签发的，才能分析可能存在的风险和提前做好具体应对对策，这是非常有价值的数

据。16917 张有效的 \*.gov.cn 域名的 SSL 证书中，各种证书类型数量和占比如下表 2 所示。从数据可以看出，政府用户也是喜欢申请无需提供任何证明材料的 DV SSL 证书，占比接近 80%。这也是我们推荐政府用户选用的证书类型，不要难为政府用户去提供无法提供的证明材料。我们很遗憾地看到不少.gov.cn 域名的 OV SSL 证书中绑定的单位名称为某某公司，这种 OV SSL 证书可能理解为错误签发的证书，还不如直接申请 DV SSL 证书。

证书类型	DV SSL 证书	OV SSL 证书	EV SSL 证书
证书数量	12,898	3,793	226
占比	76.24%	22.42%	1.34%

表 2

签发这 16917 张 SSL 证书的 SSL 证书提供商前 18 位排名及签发数量和国别如下表 3 所示，鉴于 SSL 证书控制权在于顶级根 CA，所以，我们同时列出了所有 SSL 证书提供商的顶级根证书是谁和属于哪个国家。我国拥有自己的顶级根 CA 的签发比例从上一季度的 6.29% 上升到 7.19%，国外 CA 占比仍然高达 92.81%。这一季度数据同上一季度相比，能发现两个亮点：一是国外 CA 占比在减少，这是一个好迹象；第二个亮点是自动化部署的证书数量有 5.44% 的增长。请注意：即使是我国自己的顶级根证书签发，但是否信任这些 RSA 算法根证书还是人家说了算，仍然有“连根除”的安全风险，普及商密 SSL 证书才是唯一安全上策。

排名	公司名称	国别	证书数	占比	增长%	根CA (国别)	备注
1	DigiCert	美国	8,730	51.60%	-0.92%	DigiCert (美国)	
2	亚数信息	中国	2,621	15.49%	1.04%	Sectigo/DigiCert (美国)	
3	Let's Encrypt	美国	871	5.15%	9.42%	ISRG (美国)	自动化部署
4	沃通CA	中国	735	4.34%	16.11%	Sectigo/DigiCert/Assecods (美国/波兰)	
5	中金认证	中国	707	4.18%	16.67%	CFCA (中国)	
6	数安时代	中国	610	3.61%	-5.57%	Assecods + GDCA (波兰 + 中国)	
7	北京信查查	中国	525	3.10%	28.05%	Assecods/Sectigo (波兰/美国)	
8	上海CA	中国	510	3.01%	21.72%	Assecods x UniTrust (中国)	
9	GlobalSign	日本	430	2.54%	12.57%	GlobalSign (日本)	
10	Sectigo	美国	349	2.06%	9.40%	Sectigo (美国)	
11	上海锐成	中国	227	1.34%	95.69%	Sectigo (美国)	
12	天威诚信	中国	148	0.87%	0.68%	Assecods (波兰)	
13	合肥网盾	中国	97	0.57%	31.08%	Sectigo (美国)	
14	腾讯云	中国	55	0.33%	-1.79%	Sectigo (美国)	
15	Cloudflare	美国	49	0.29%	-16.95%	DigiCert (美国)	自动化部署
16	北京新网	中国	42	0.25%	-6.67%	Sectigo (美国)	
17	ZeroSSL	奥地利	38	0.22%	-17.39%	Sectigo (美国)	
18	深圳CA	中国	30	0.18%	-18.92%	Assecods (波兰)	
19	其他		143	0.85%	107.25%	国外CA	
合计			<b>16,917</b>				

表 3

我们同时还检索了港澳台地区的 SSL 证书申请量，如下表 4 所示。我国大陆各省市所有政府网站合计证书申请量为 **16917** 张，连续三个季度超过港澳台的数据的总和，这说明了我国大陆地区的政府网站已经开始重视网站信息安全防护和数据加密保护工作。

	数量	增长%	检索域名	默认https	启用国密	WAF防护	安全评级
中国大陆	<b>16917</b>	3.90%	*.gov.cn	是	否	有	B+
中国台湾省	<b>12534</b>	0.41%	*.gov.tw	是	否		B+
中国香港特别行政区	<b>2023</b>	1.30%	*.gov.hk	是	否		B+
中国澳门特别行政区	<b>437</b>	-0.68%	*.gov.mo	是	否		B+

表 4

### 三、我国本土国际 SSL 证书提供商的统计数据分析

我国本土国际 SSL 证书提供商的证书签发数量统计数据同样来自谷歌证书透明日志系统，真实可信，能准确反映我国本土国际 SSL 证书的提供能力和市场情况。“国际 SSL 证书”是指目前正在大量使用的采用国际算法 RSA 或 ECC 的 SSL 证书。“本土 SSL 证书提供商”是指证书签发中级根证书的 O 字段的国家是“CN(中国)”的机构，而之所以称之为“SSL 证书提供商”，这是参考了国际上通用的名称-SSL Certificate Provider，可简称为“SCP”，SSL 证书作为一个互联网安全产品在国外并没有被定义为必须是 CA 机构才能提供，目前全球 SSL 证书市场份额排名前十的 SCP 中只有 2 家是专门签发证书的 CA 机构，仅排名为第六和第七，其余都是全球知名的互联网和云服务提供商。

如下表 5 所示，本次列入统计的本土 SSL 证书提供商有 18 家，都是拥有自主品牌的全球信任的 SSL 中级根证书的证书提供商，其他仅仅是某个品牌的代理商并不在统计之列。这 18 家 SSL 证书提供商中有 8 家公司是 CA 机构，有 3 家是知名的云服务提供商，其他 7 家是商业公司。

而这 18 家国际 SSL 证书提供商中，拥有自主顶级根证书并用于签发国际 SSL 证书的只有 3 家 CA 机构：

中金认证、上海 CA 和数安时代，其中上海 CA 的根证书同波兰 CA 做了交叉签名(下表中表示为“x”)，数安时代同时从定制中级根和自主根签发证书(下表中表示为“+”)。其他 15 家证书提供商的 SSL 证书都是从国外 CA 定制品牌中级根证书签发，主要是美国 CA-Sectigo、DigiCert 和波兰 CA-Assecods，本季度新增一家-新网数码，唯一一个从国内 CA 机构定制了中级根证书的 SSL 证书提供商。

这 18 家国际 SSL 证书提供商签发的有效证书数合计为 **127.4870** 万张，比上一季度减少了 **1.52%**，对比全球数据增加了 **10.10%**，国内 SSL 证书提供商的市场份额连续三个季度在下降，这 18 家的总和在全球 SSL 证书提供商中排名第 **14** 位。而排名前 10 位的 SSL 证书提供商都在为用户提供自动化证书管理服务，用户喜欢能提供自动化申请和部署的 SSL 证书提供商，希望国内 SSL 证书提供商能尽快为用户提供自动化证书管理服务，特别是应该提供国密证书自动化管理服务，以实现双算法双 SSL 证书的自动化管理。国际 SSL 证书是临时市场，而国密 SSL 证书则是未来市场，早投入早收益。值得一提的是：合肥网盾在本季度跻身前 5 名，其增长秘诀是实现了自动化证书管理。零信证签在本季度增长了 144.23%，这是由于已经有用户开始使用零信国密 HTTPS 加密自动化解决方案实现 HTTPS 加密自动化。这些都是自动化的威力，用户需要自动化证书管理。

排名	公司名称	证书签发量	增长%	顶级根
1	亚数信息	1,197,722	-3.21%	Sectigo/DigiCert
2	上海锐成	19,987	98.64%	Sectigo
3	北京信查查	14,457	12.18%	Assecods/Sectigo
4	沃通CA	10,471	11.06%	Sectigo/Assecods/DigiCert
5	合肥网盾	5,704	43.86%	Sectigo
6	腾讯云	4,992	10.93%	Sectigo
7	上海CA	4,350	21.00%	Assecods x UniTrust
8	中金认证	4,056	6.76%	CFCA
9	零信证签	3,766	144.23%	Sectigo
10	天威诚信	2,485	8.99%	Assecods
11	数安时代	1,301	0.46%	Assecods + GDCA
12	北京新网	1,270	-6.00%	Sectigo
13	百度云	981	3.15%	Sectigo
14	阿里云	961	111.67%	GlobalSign
15	浙江葫芦娃	818	5.55%	Sectigo
16	新网数码	482		UniTrust
17	北京中万	207	13.11%	Sectigo
18	深圳CA	202	40.28%	Assecods
	其他	658		
合计		<b>1,274,870</b>	<b>-1.52%</b>	

表 5

#### 四、我国国密 SSL 证书提供商的统计数据分

本期发布的国密 SSL 证书数据来自零信国密证书透明日志系统([sm2ct.cn](http://sm2ct.cn))和来自主动上报的各个零信浏览器信任的 CA 机构，由于各家 CA 上报的数据无法核实是否可信，所以，本次报告的国密 SSL 证书数据仅供参考。合计 **4329** 张，比上一季度增长了两倍多(**204.39%**)，这是一个可喜的数据，说明我国的国密改造工作正在如火如荼进行中，一个重要的案例就是深圳政府在线已经完成国密改造，实现了深圳政府门户网站的国密 HTTPS 加密保护。

另一个值得在此一提的大事是密标委已经下文由零信技术牵头制定证书自动化商密标准-《自动化证书管理规范》和证书透明商密标准-《证书透明规范》，这两个标准制定的立项成功标志着国密 SSL 证书透明已经有标准可依了，证书透明和证书自动化将驶入发展快车道，将为保障商密 SSL 证书的可靠供给和普及应用提供标准支撑，将加速商密 SSL 证书的普及应用部署，加速采用商用密码来保障我国网络空间安全。

为此，零信浏览器把计划强制实施国密证书透明计划的日期从原计划的 2024 年 1 月 1 日推迟到 2024 年 7 月 1 日，让各家国密 CA 机构有足够的时间去升级 CA 系统支持国密证书透明。从 2024 年 7 月 1 日起，

零信浏览器会采用谷歌浏览器一样的证书透明策略,对没有在国内证书透明日志系统公开披露的国密 SSL 证书标记为不可信的 SSL 证书,请各家 CA 机构抓紧时间对接零信国密证书透明日志系统。

当然,我们希望有更多机构,包括国家密码主管部门和国家网站管理部门,能提供更加权威的国密证书透明日志服务。只有所有 CA 机构签发的国密 SSL 证书都像国际 SSL 证书一样都提交到证书透明日志系统,国密 SSL 证书的签发统计数据才是真实的数据,国密 SSL 证书才能保障自身安全,才能真正可靠地实现国密 HTTPS 加密,以保障我国网站系统安全。

## 五、全球十大 SSL 证书提供商排名变化分析与启示

本期数据是 2023 年的年终数据,我们回顾一下这一年来全球前十大 SSL 证书提供商的排名变化情况,从中可以发现我国 SSL 证书提供商的发展思路,这个最有价值。如下表 6 所示,Let's Encrypt 稳居第一位,并且首次超过了 50%市场份额,其成功秘诀在于它是首家提供自动化证书管理服务的厂商,是一个浏览器背景的软件厂商,不仅自动化提供免费 90 天 SSL 证书,而且牵头制定了 RFC8555 国际标准,使得大量的服务提供商都依据标准对接其自动化证书服务系统,自动化为各种业务系统和各种物联网设备部署 SSL 证书。也就是说,LE 由于成功打造了自动化证书管理生态,大家都离不开这个生态了,其市场份额只会是一直不断增长,其证书量是排名第二谷歌的 5.42 倍,比其他 9 位的总和还要多。

	Q1排名	Q2排名	Q3排名	Q4排名
1	Let's Encrypt	Let's Encrypt	Let's Encrypt	Let's Encrypt
2	Cloudflare	Cloudflare	Cloudflare	谷歌
3	亚马逊	谷歌	谷歌	亚马逊
4	谷歌	亚马逊	亚马逊	Cloudflare
5	Sectigo	Sectigo	Sectigo	GoDaddy
6	DigiCert	DigiCert	DigiCert	Sectigo
7	微软	微软	GoDaddy	DigiCert
8	cPanel	cPanel	微软	ZeroSSL
9	GoDaddy	GoDaddy	ZeroSSL	微软
10	ZeroSSL	ZeroSSL	cPanel	cPanel

表 6

第二个值得关注的是谷歌信任服务,从 2022 年 3 月 30 日开始提供 ACME 服务,到 2023 年 4 月 1 日一年时间从零开始一跃成为全球排名第四位的 SSL 证书提供商,第二季度就上升到第三位,而第四季度又升到到了第二位,也就是说谷歌只用了一年零九个月就成为了全球老二。取得这样的业绩的主要原因有三个:第一是互联网公司和云服务商拥有大量的用户,一旦谷歌能为这些云服务免费自动化提供 SSL 证书,用户当然就用谷歌的自动化证书服务了;第二是谷歌拥有自己的顶级根证书,能完全自主可控地为用户可靠地提供 SSL 证书自动化签发服务,连原排名第二位的 Cloudflare 也开始为用户自动化配置谷歌签发的 SSL 证书而不是自己品牌的 SSL 证书;第三是谷歌浏览器的绝对市场份额(超过 70%),让用户也愿意选择谷歌的自动化证书服务,因为谷歌自己签发的 SSL 证书谷歌浏览器绝对是会信任的,而选择其他家则有可能遭遇不被信任的风险。这三个原因使得大家愿意用其自动化证书管理服务,其市场份额就自然而然地飞速提升。亚马逊的成功也可以归类到谷歌的成功模式中,虽然它没有浏览器,但是有第一和第二个原因一样的优势。

第三个值得关注的 Cloudflare 和微软,这两家可以放在同一类分析。这两家的共同点是都没有自己的顶级根证书,都是从其他 CA 机构定制了 SSL 中级根证书,不仅仅是费用问题,更重要的是会受到顶级根 CA 的技术制约和性能制约,因为用户证书的验证和签发必须由顶级根 CA 来负责。也许正是这个原因使得

Cloudflare 不惜牺牲自己品牌的签发数据而选择为用户自动化配置谷歌签发的 SSL 证书，这里也能体会到 Cloudflare 真正为用户着想的服务理念。这两家公司都是云服务提供商，也一样拥有大量的需要 SSL 证书的用户。cPanel 也可以归类到这一类(没有自己的根证书)，其根本原因是用户可能不再需要其核心产品 cPanel，虽然仍然有大量用户。

第四个值得关注的是 Sectigo 和 DigiCert，全球前两大 CA 机构理应排名第一和第二，但由于没有及时为用户提供自动化证书管理服务，而在本季度分别从排名第 5 和第 6 位下降到第 6 和第 7 位。虽然这两家 CA 已经开始提供自动化证书管理服务，但是由于仅提供证书服务，用户已经在云服务提供商那里自动化拿到了 SSL 证书，怎么还会向你申请证书？目前的市场份额应该基本上都是传统的人工申请证书的用户的申请量，随着用户直接使用云服务平台的 SSL 证书，预计 2024 年还会继续下滑。

第五个值得关注的是 GoDaddy，这是一家老牌域名注册服务提供商，拥有大量的域名注册用户，这家公司陆续提供了各种云服务和成为 CA 机构并拥有自己的顶级根证书，使其能为域名用户提供自动化证书服务，其排名从第一季度的第 9 位一路快速上升到第三季度的第 7 位和第四季度的第 5 位。这个成功模式非常值得国内所有域名注册服务提供商学习与借鉴，这是为何单独列为一类的原因，其实也可以归类到第二种情况中，即云服务厂商拥有大量的 SSL 证书需求用户，用户需要一站式解决方案提供商。

## 六、统计数据亮点和问题分析

本期统计数据的亮点是国密 SSL 证书申请量的两倍增长，因为大量的国密改造需要国密 SSL 证书。但是，传统的向 CA 申请国密 SSL 证书的方案对于少量几个网站的国密改造尚能接受，而对于一个省级政务云平台有上万个网站需要完成国密 HTTPS 加密改造，手动申请国密 SSL 证书，并改造 Web 服务器支持国密算法的改造方案根本行不通，唯一的解决方案是零改造的部署国密 HTTPS 加密自动化网关，实现国密 SSL 证书的自动化申请和部署，原 Web 服务器零改造就可以完成国密改造，这才是唯一可行的方案。

## 七、小结

本期报告在新年假期完成，2023 年我国已经完成了商密 SSL 证书所需的所有商密标准的立项制定工作，相关公司已经完成了整个生态所需的所有商密 SSL 证书的可靠生产和快速部署的产品研发工作，2023 年已经实现了年初我们定位的“国密 HTTPS 加密普及元年”，我们把 2024 年定为“国密 HTTPS 加密自动化年”，今年极有可能落地 90 天有效期 SSL 证书安全政策，唯有自动化才能实现国密 HTTPS 加密的普及应用。唯有拥抱自动化，才能适应不断变化的网络安全浪潮，在数字时代实现稳健增长。

新年新气象，为了应对不确定的国际环境，我国只有普及应用商密 HTTPS 加密才能保障我国网络空间安全，这是网络空间安全的基础安全保障，保障了网站安全也就是保护了国家安全，因为“没有网络安全就没有国家安全”。而只有保障了国家安全，才会有小家的岁岁年年享受阖家团圆，才能享受畅游美好的祖国山山水水。

祝福所有读者，感谢广大读者一年来对中国 SSL 证书市场发展趋势分析简报的关爱，2024 年我们将加强数据的深度分析，提供更细分粒度的相关数据，为相关产业发展提供决策数据支撑。

**零信技术零信任安全研究院**

2024 年 1 月 2 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。  
从 2021 年 12 月 9 日开始，已累计发表 207 篇，共 38 万多字中文和 7 万多英文单词。

