中国 SSL 证书市场发展趋势分析简报-2024Q4

2025 年 1 月 3 日

本报告由**零信任安全研究院**和**零信浏览器**全球独家联合发布，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 2024 年第 4 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 签发的国际 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和产业发展政策。

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 **2024 年 12 月 31 日**，已经在国际证书透明日志系统记录的未过期的全球信任的 SSL 证书有 **10.3194** 亿张，比上一季度增加了 **16.46%**，其中只验证域名的 DV SSL 证书、验证单位身份的 OV SSL 证书和扩展验证单位身份的 EV SSL 证书的签发量、占比和同上一季度环比数据如下表 1 所示，本季度的 OV SSL 证书占比比一季度增加了 1.10%，说明微软云、Cloudflare 和思科等大厂自动化签发了大量的 O 字段为其公司名称的 OV SSL 证书的签发量有增加，实际上是为使用其云服务的网站和设备签发的，也就是说 ACME 自动化签发不仅仅适用于 DV SSL 证书，也可用于 OV SSL 证书和 EV SSL 证书。

	DV SSL证书	OV SSL证书	EV SSL证书
签发量	930,781,507	100,577,971	338,129
占比	90.20%	9.75%	0.03%
环比增长	15.05%	31.22%	-7.23%

表 1

全球 **10.3194 亿**张有效证书中，排名前十五大 SSL 证书提供商的证书签发量、占比和同上季度环比增长情况如下表 2 所示，第 1 位仍然是 Let's Encrypt，并且比上一季度增加了 12.90%，市场占比比上季度略有下降，第 2 位是谷歌，比上一季度上升了一位，GoDaddy 排名第 3，下降了一位。值得一提的是传统 CA 机构 DigiCert 保持在第 4 位，环比增长 20.71%，说明 DigiCert 已经发力自动化证书管理，这值得所有国内 CA 机构学习和借鉴。

(C) 2025 零信技术（深圳）有限公司

排名	公司名称	签发量	占比%	环比%	Q3排名	公司类型	国别
1	Let's Encrypt	470,766,707	45.62%	12.90%	1	互联网软件	美国
2	谷歌	157,617,432	15.27%	48.90%	3	互联网公司	美国
3	GoDaddy	111,210,868	10.78%	0.79%	2	域名注册商	美国
4	DigiCert	85,886,230	8.32%	20.71%	4	CA机构	美国
5	微软	68,705,002	6.66%	81.18%	6	云服务提供商	美国
6	亚马逊	59,808,902	5.80%	-1.35%	5	云服务提供商	美国
7	Sectigo	37,740,932	3.66%	4.08%	7	CA机构	美国
8	ZeroSSL	13,618,315	1.32%	-18.68%	8	SSL证书提供商	奥地利
9	Cloudflare	9,644,817	0.93%	-25.65%	9	CDN服务提供商	美国
10	IdenTrust	3,666,238	0.36%	18.98%	11	CA机构	美国
11	cPanel	3,075,480	0.30%	-26.97%	10	软件提供商	美国
12	思科	2,365,365	0.23%	11.68%	12	网络设备制造商	美国
13	GlobalSign	1,539,428	0.15%	-0.26%	13	CA机构	日本
14	亚数信息	954,671	0.09%	-17.96%	14	SSL证书提供商	中国
15	Actalis	851,145	0.08%	-12.10%	15	CA机构	意大利
16	其他	4,494,856	0.44%	33.32%			
	合计	**1,031,946,388**					**2024Q4**

表 2

本期继续直接采用表格形式列出全球前 15 大 SSL 证书提供商的情况，主要是希望用户能了解全球 SSL 证书市场的全貌，这 15 大中美国不仅占据前 7 大，而且共有 11 家，占比 73%，证书签发量占 97.92%。我国有一家，但并不是顶级根 CA，而是定制美国 CA 的中级根 SSL 证书提供商，已连续两个季度都是两位数的负增长。展示公司类型的目的是希望给我国各相关行业领导者战略决策参考，一定要改变只有 CA 机构才能签发 SSL 证书的传统旧观念！比如说，互联网软件厂商就应该向 LE 学习，LE 就是编写一个自动化申请证书的软件而一跃成为全球第一大 SSL 证书提供商，并且拥有自己顶级根的 CA 机构。还有互联网公司、云服务提供商、设备制造商等等，都可以通过定制中级根方式来实现自动化为用户提供自己品牌的 SSL 证书，从而实现行业逆袭。

如下图 1 所示，用圆饼图直观展示全球前 15 大 SSL 证书提供商的证书签发量排名和占比情况。

(C) 2025 零信技术（深圳）有限公司

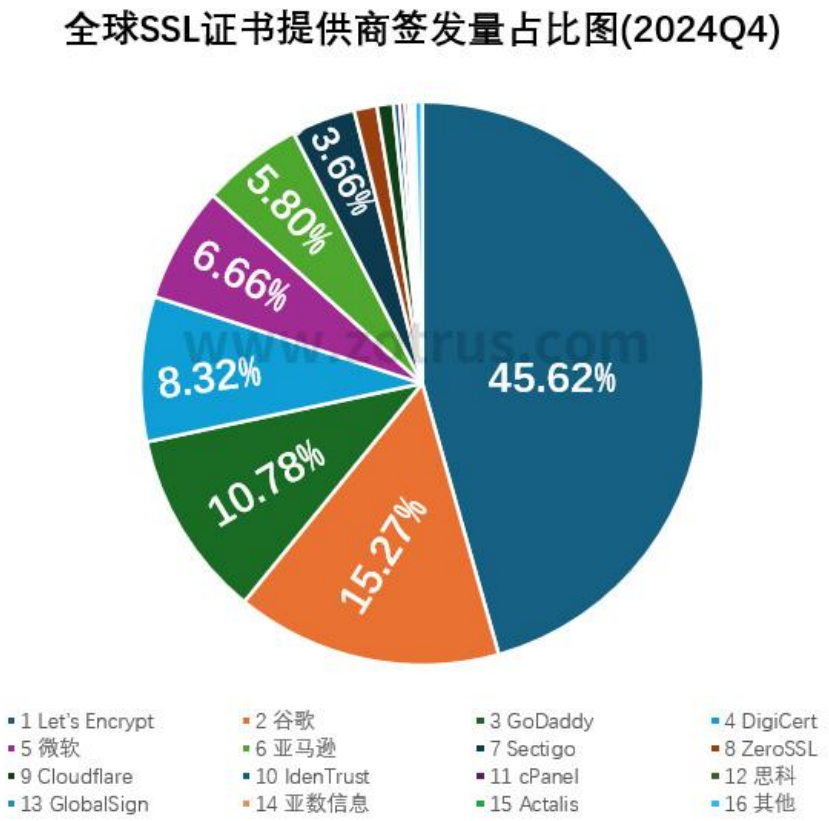

图 1

本季度的数据中的 DV SSL 证书比例高达 90%，这个数据非常值得重视，因为谷歌在去年 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，苹果于去年 10 月提出了缩短为 45 天。谷歌和苹果发布这些计划是有底气，因为目前全球有效 SSL 证书中已经有 90%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 证书统计数据分析

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

(C) 2025 零信技术（深圳）有限公司

两个域名的 SSL 证书申请数量。

具体数据如下表 3 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 **1779** 张，比上一季度减少了 **1.22%**，这是在连续三个季度增长后减少。其中，排名前 5 名本季度没有变化，仍然是**上海市、浙江省、北京市、海南省、广西壮族自治区**，值得注意的是本季度有 14 个省市自治区为负增长。

排名	省市自治区	数量	增长%	占比%	检索域名	默认https	部署国密	WAF防护	安全评级
1	上海市	267	-2.20%	15.01%	shanghai.gov.cn, sh.gov.cn	是	否		B+
2	浙江省	149	-9.15%	8.38%	zj.gov.cn	是	否		B
3	北京市	122	-4.69%	6.86%	beijing.gov.cn	是	否	有	B+
4	海南省	114	2.70%	6.41%	hainan.gov.cn	是	否		B+
5	广西壮族自治区	91	-5.21%	5.12%	gxzf.gov.cn	否	否		
6	宁夏回族自治区	77	5.48%	4.33%	nx.gov.cn	是	否	有	B+
7	广东省	72	0.00%	4.05%	gd.gov.cn	否	否		
8	天津市	71	1.43%	3.99%	tj.gov.cn	是	否	有	B+
9	山东省	69	2.99%	3.88%	shandong.gov.cn, sd.gov.cn	否	否		
10	云南省	61	-8.96%	3.43%	yn.gov.cn	是	否		B+
11	河南省	56	-6.67%	3.15%	henan.gov.cn	是	否		B+
12	甘肃省	51	4.08%	2.87%	gansu.gov.cn	是	否		B+
13	贵州省	51	4.08%	2.87%	guizhou.gov.cn	否	否		
14	吉林省	47	6.82%	2.64%	jl.gov.cn	否	否		
15	江西省	46	4.55%	2.59%	jiangxi.gov.cn	否	否		
16	黑龙江省	44	2.33%	2.47%	hlj.gov.cn	是	否	有	B+
17	湖南省	43	7.50%	2.42%	hunan.gov.cn	是	是		A
18	重庆市	42	0.00%	2.36%	cq.gov.cn	否	否		
19	陕西省	40	0.00%	2.25%	shaanxi.gov.cn	是	是		B+
20	安徽省	38	-9.52%	2.14%	ah.gov.cn	是	否	有	B+
21	河北省	36	-5.26%	2.02%	hebei.gov.cn	否	否		
22	青海省	36	16.13%	2.02%	qinghai.gov.cn	否	否		
23	新疆维吾尔自治区	32	-3.03%	1.80%	xinjiang.gov.cn	是	否		B+
24	辽宁省	30	20.00%	1.69%	ln.gov.cn	是	否		B+
25	江苏省	21	-8.70%	1.18%	jiangsu.gov.cn, js.gov.cn	否	否		
26	福建省	20	-9.09%	1.12%	fujian.gov.cn, fj.gov.cn	是	否		B+
27	西藏自治区	20	5.26%	1.12%	xizang.gov.cn	否	否		
28	内蒙古自治区	11	-15.38%	0.62%	nmg.gov.cn	是	否		B+
29	山西省	10	-9.09%	0.56%	shanxi.gov.cn	否	否		
30	湖北省	9	12.50%	0.51%	hubei.gov.cn	否	否		
31	四川省	3	-25.00%	0.17%	sc.gov.cn	是	否		B+
	合计	1779	-1.22%			18	2	5	2024Q4

表 3

对于国密算法 SSL 证书的部署情况，本季度新增了陕西省，但海南省证书过期没有续期，所以 31 个省市自治区省级政府官网中部署了商密 SSL 证书的还是两个省：湖南省和陕西省。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国密 HTTPS 加密自动化网关，原系统零改造，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 18 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

(C) 2025 零信技术（深圳）有限公司

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，能节省原服务器的 20%-30%算力，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 5 个省政府网站有 WAF 防护，同时启用了默认 https 加密，只有这样，WAF 防护才真正发挥防护作用。当然，我们无法知道政府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。

如下图 2 所示，用圆饼图直观展示全国 31 个省市自治区政府网站的证书签发量排名和占比情况。

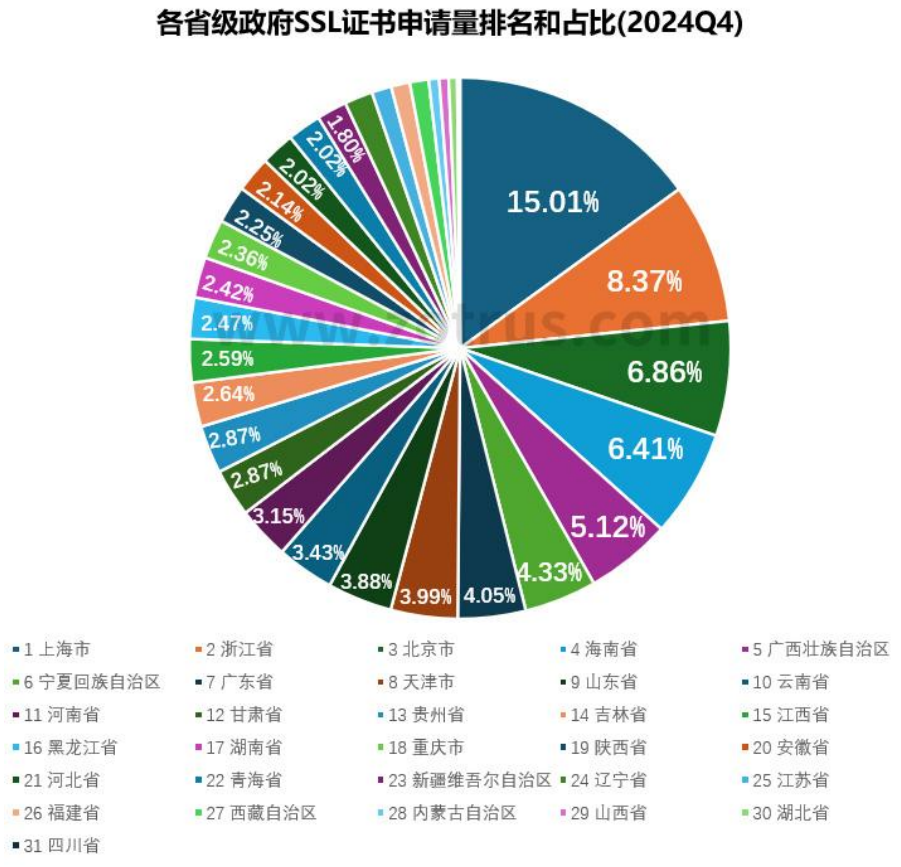

图 2

我们检索了***.gov.cn** 的 SSL 证书申请量为 **16522** 张，比上一季度减少了 **4.81%**，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 1779 张。这些*.gov.cn 域名的 SSL 证书中，各种证书类型数量和占比如下表 4 所示。从数据可以看出，政府用户仍

(C) 2025 零信技术（深圳）有限公司

然喜欢申请无需提供任何证明材料的 DV SSL 证书，占比 68.73%，比上期有所下降。而需要提供身份认证证明材料的 OV SSL 证书的占比继续上升中，推荐政府用户向国内 CA 机构申请 OV 或 EV SSL 证书，如果要申请国外 CA 机构签发的 SSL 证书，则推荐申请 DV SSL 证书，以避免数据出境管理风险。但是，我们发现，多个省市的政府官网的 OV SSL 证书的 O 字段并不是政府机构名称，而且公司名称，这绝对是一张错误签发的 OV SSL 证书，可以理解为是销售商为了提高证书销售额但又拿不到政府机构的身份证明材料的无奈之举和不良行为，应该直接给这些政府网站申请 DV SSL 证书，而不是给一张身份信息错误的 OV SSL 证书。

	DV SSL证书	OV SSL证书	EV SSL证书
签发量	11356	4954	212
占比	68.73%	29.98%	1.28%
环比	-5.74%	-2.46%	-7.42%

表 4

为政府网站*.gov.cn 签发这 **16522** 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 5 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。对比上一期数据可以看出：美国 CA-DigiCert 下降了 13%，这是连续 6 个季度在下降，可以看出政府用户更加青睐国内 CA。

排名	公司简称	证书数	占比	增长%	国别	根CA (国别)
1	DigiCert	5146	31.15%	-12.79%	美国	DigiCert (美国)
2	亚数信息	2304	13.95%	-21.28%	中国	Sectigo/DigiCert (美国)
3	Let's Encrypt	1667	10.09%	9.17%	美国	ISRG (美国)
4	中金认证	1127	6.82%	-14.17%	中国	CFCA (中国)
5	沃通CA	1048	6.34%	12.33%	中国	Sectigo/DigiCert/Assecods (美国/波兰)
6	北京信查查	879	5.32%	14.60%	中国	Assecods/Sectigo (波兰/美国)
7	上海CA	750	4.54%	5.93%	中国	Assecods x UniTrust (中国)
8	Sectigo	588	3.56%	18.07%	美国	Sectigo (美国)
9	上海锐成	585	3.54%	12.72%	中国	Sectigo (美国)
10	数安时代	580	3.51%	-3.65%	中国	Assecods/GDCA (波兰/中国)
11	GlobalSign	440	2.66%	-7.95%	日本	GlobalSign (日本)
12	ZeroSSL	281	1.70%	21.12%	奥地利	Sectigo (美国)
13	天威诚信	198	1.20%	5.88%	中国	Assecods (波兰)
14	合肥网盾	189	1.14%	30.34%	中国	Sectigo/UniTrust/Assecods (美国/中国/波兰)
15	新网数码	186	1.13%	18.47%	中国	Sectigo (美国)/UniTrust (中国)
16	腾讯云	105	0.64%	40.00%	中国	Sectigo (美国)
17	Assecods	46	0.28%	21.05%	波兰	Assecods (波兰)
18	Google TS	16	0.10%		美国	Google (美国)
	其他	387	2.34%	10.89%		国外CA
合计		16,522		-4.81%		2024Q4

表 5

(C) 2025 零信技术（深圳）有限公司

如下图 3 所示，用圆饼图直观展示为我国政府网站的签发国际 SSL 证书的 SSL 证书提供商的排名和占比情况。

图 3

我们同时还检索了港澳台地区的 SSL 证书申请量，如下表 6 所示。我国大陆各省市所有政府网站合计证书申请量为 **16522** 张，仍然比台湾省的证书申请量少，本季度大陆和港澳台地区政府网站的 SSL 证书申请量全都有不同幅度的减少。

	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	16,522	-4.81%	*.gov.cn	是	否	有	B+
中国台湾省	20,054	-21.88%	*.gov.tw	是	否		B+
中国香港特别行政	2,789	-2.35%	*.gov.hk	是	否		B+
中国澳门特别行政	471	-7.83%	*.gov.mo	是	否		B+

表 6

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”是指证书的中级根证书的 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

(C) 2025 零信技术（深圳）有限公司

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 3 家是 CA 机构，仅排名为第四、第七和第十，其余都是全球知名的互联网巨头和云服务提供商。

如下表 7 所示，本次列入统计的本土 SSL 证书提供商有 17 家，都是拥有自主品牌的全球信任的 SSL 中级根证书的 SSL 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 17 家 SSL 证书提供商中有 7 家公司是 CA 机构，有 3 家是知名的云服务提供商，其他 8 家是商业公司。

而这 17 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。其他 14 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。

这 17 家国际 SSL 证书提供商签发的有效证书数合计为 **117.8151** 万张，比上一季度下降了 **12.98%**，对比全球数据增加了 **16%**，国内 SSL 证书提供商的市场份额已连续两个季度都在下降，这 17 家的总和在全球 SSL 证书提供商中排名仍然是第 **14** 位。本期虽然总数有下降，但是多家机构的增幅超过 20%，有两家超过 60%，这里面一定是在自动化证书管理方面的努力结果，值得点赞。对比上一季度数据，亚数虽然还保持第一位，但是连续两个季度两位数的负增长，本季度首次跌破 100 万张，这个值得注意。零信证签又上升了一位，新网数码上升了两位，上海环度上升了 3 位，中金认证下降了两位。

排名	公司简称	签发量	增长%	占比%	根CA (国别)
1	亚数信息	957,026	-17.94%	81.23%	Sectigo/DigiCert (美国)
2	上海锐成	93,115	27.53%	7.90%	Sectigo (美国)
3	沃通CA	32,719	39.66%	2.78%	Sectigo/DigiCert/Assecods (美国/波兰)
4	北京信查查	23,160	12.08%	1.97%	Assecods/Sectigo (波兰/美国)
5	零信证签	14,175	-8.38%	1.20%	Sectigo/UniTrust (美国/中国)
6	合肥网盾	11,553	-26.06%	0.98%	Sectigo/UniTrust/Assecods (美国/中国/波兰)
7	腾讯云	8,912	28.60%	0.76%	Sectigo (美国)
8	新网数码	8,396	67.89%	0.71%	Sectigo (美国)/UniTrust (中国)
9	上海CA	6,721	8.26%	0.57%	Assecods x UniTrust (中国)
10	中金认证	5,873	-12.34%	0.50%	CFCA (中国)
11	天威诚信	4,640	7.23%	0.39%	Assecods (波兰)
12	阿里云	3,849	19.02%	0.33%	GlobalSign (日本)
13	上海环度	1,817	70.13%	0.15%	UniTrust (中国)
14	浙江葫芦娃	1,756	21.27%	0.15%	Sectigo (美国)
15	数安时代	1,359	-0.73%	0.12%	Assecods/GDCA (波兰/中国)
16	百度云	1,055	-26.02%	0.09%	Sectigo (美国)
17	厦门纳网	647	13.11%	0.05%	Sectigo (美国)
18	其他	1,378	12.77%	0.12%	
合计		**1,178,151**	**-12.98%**		**2024Q4**

表 7

(C) 2025 零信技术（深圳）有限公司

本期合计统计 **117 万**多张 SSL 证书中各种类型的占比数据如下表 8 所示，DV SSL 证书占比高达 **97.35%**，这个比例比全球市场的 DV SSL 证书的占比 90%高出不少，这说明了我国用户比全球用户更加喜欢无需提供任何身份证明材料的 DV SSL 证书，因为目前用户不愿意提供身份认证材料给国外 CA，认证审核时间长和存在数据出境管理风险，这也可能是政府用户选择向国内 CA 申请 OV/EV SSL 证书的主要原因。

	DV SSL证书	OV SSL证书	EV SSL证书
数量	1,146,919	30,094	1,138
占比	97.35%	2.55%	0.10%

表 8

四、 我国国密 SSL 证书提供商的统计数据分析

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 **47033** 张，比上一季度增长了 **58%**，连续 9 个季度持续快速增长，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，增长最多的是网银系统用国密 SSL 证书，其次是政府网站和政务服务系统。

本季度无新增 CA 机构支持国密证书透明标准草案，希望更多了零信浏览器信任的 CA 机构签发的国密 SSL 证书支持国密证书透明，一旦有 5 家 CA 机构签发的国密 SSL 证书支持国密证书透明标准草案，本报告将像国际 SSL 证书一样列表排名各个商密 SSL 证书提供商签发的商密 SSL 证书，以帮助用户在选购商密 SSL 证书时优先选择支持国密证书透明的商密 SSL 证书提供商，从而保障用户自身的合法权益和网站安全。证书透明，向全世界告白-这张证书是我签发的，能大大提升 SSL 证书提供商的品牌知名度！

我们希望有更多机构，包括国家相关管理部门，能提供更加权威的国密证书透明日志服务。只有所有 CA 机构签发的商密 SSL 证书都像国际 SSL 证书一样都提交到证书透明日志系统，商密 SSL 证书的签发统计数据才是真实的数据，商密 SSL 证书才能真正保障其自身安全，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、 2024 年度数据汇总分析

如火如荼的 2024 年已经过去了，让我们通过下表对比看看这一年来几个重要数据的变化。

(C) 2025 零信技术（深圳）有限公司

	2023 年 Q4	2024 年 Q4	增长率
国际 SSL 证书总数	6.7644 亿张	10.3194 亿张	52.55%
国际 DV SSL 证书占比	85.52%	90.20%	5.47%
国内 SSL 证书提供商证书总数	127.4870 万张	117.8151 万张	-7.59%
*.gov.cn 国际 SSL 证书数	16917 张	16522 张	-2.33%
31 个省市自治区政府域名 国际 SSL 证书申请总数	1555 张	1779 张	14.41%
31 个省市自治区政府域名 国际 DV SSL 证书占比	76.24%	68.73%	-9.85%
31 个省市自治区政府官网 默认 HTTPS 加密	18 个	18 个	0.00%
国密 SSL 证书总数	4329 张	47033 张	**1086.46%**
31 个省市自治区政府官网 国密 HTTPS 加密	1	2	100%

表 9

从上表各种数据可以看出：

(1) 全球 SSL 证书增长率为 52%，但我国政府网站的 SSL 证书增长率只有 14%，远低于全球增长率。

(2) 虽然全球 SSL 证书申请量增长了 52%，但是我国本土 SSL 证书提供商的证书总数却下降了 8%，说明国际 CA 在国内的市场占有率有所提升，主要是支持 ACME 自动化部署的 LE 和 GTS 的市场份额正在快速上升，这非常值得国内 SSL 证书提供商高度重视，用户喜欢自动化部署。

(3) 我国政府网站(*.gov.cn)SSL 证书申请量下降了 2.33%，而总数 16522 张只占我国政府事业单位网站标识发放总量 109310 的 15.11%，说明还有大量的政府网站没有部署 SSL 证书。

(4) 国际 SSL 证书中只验证域名的 DV SSL 证书占比增长了 5.47%，相比我国政府市场，反而下降了将近 10%，这说明政府市场比国际市场更青睐验证身份的 OV SSL 证书和 EV SSL 证书，这一点也值得国内 SSL 证书提供商和销售商注意。

(5) 31 个省市自治区政府官网默认 HTTPS 加密比例只有 58%，并且一年来没有增长，这同欧美政府网站都是 100% 默认 HTTPS 加密相比，还有巨大的改进空间。主要障碍还是传统的人工部署 SSL 证书很繁琐，应当尽快实现 SSL 证书自动化部署。

(6) 国密 SSL 证书申请量增长了将近 11 倍，这是一个大亮点，说明随着相关国密合规的法律法规的健全和完善，执法检查力度越来越大，国密 SSL 证书市场将在 2025 年有爆发式增长。但是，相比 31 个省市自治区政府官网只有两个省部署了国密 SSL 证书，并且只有一个省是默认启用国密 HTTPS 加密，这更加说明了国密改造有多难！推荐普及应

(C) 2025 零信技术（深圳）有限公司

用零改造的国密 HTTPS 加密自动化管理解决方案。

(7) 国密 SSL 证书从 2023 年 Q4 的 4 千多张，到 2024 年 Q4 的 4 万多张，对比全球国际 SSL 证书已经有了 10 亿多张，可见市场潜力巨大。再对比我国本土国际 SSL 证书提供商签发了 117 万多张，只要国内 SSL 证书提供商都能像零信证签一样为用户默认签发双算法 SSL 证书，那 2025 年国密 SSL 证书的签发量就可达到百万张，增长幅度就是 25 倍。由此可预见国密 SSL 证书的市场潜力是非常大的。

六、 2024 年 SSL 证书相关法规分析

2024 年我国相关部门发布了多个与 SSL 证书和 HTTPS 加密相关的法规文件，最值得关注的有 3 个：

(1) 5 月 22 日，网信办、中央编办、工信部和公安部联合发布了《互联网政务应用安全管理规定》，要求所有政府网站和政务服务系统都必须实现国密 HTTPS 加密方式安全连接，此规定从 7 月 1 日起施行，包括所有关键信息基础设施单位运行的所有互联网应用。这个规定的力度还是很大的，明确指出对于没有实现的单位将依规依纪追究当事人和有关领导的责任。

这对于这些单位来讲是一项艰巨的任务，而对于相关服务提供商来讲则是一个巨大的市场机会，因为根据上面的统计数据，政府网站的 SSL 证书申请量只占网站总数的 15%。但是，这个市场绝对不是简单的销售 SSL 证书市场，而且要为政府用户提供国密 HTTPS 加密自动化解决方案。

(2) 7 月 19 日，国家密码管理局发布了《国家密码管理局商用密码随机抽查事项清单(2024 年版)》，这可以理解为这是对 5 月 22 日四部委发布的《规定》的监督检查执法，采用抽查方式来检查，威慑力更大。11 月 15 日还发布了关于《关键信息基础设施商用密码使用管理规定（征求意见稿）》公开征求意见的通知，这个就是要专门针对关键信息基础设施运营单位出台更加严格的国密合规管理规定。

这对于政府、金融、电信等关键信息基础设施运营单位来讲，也是一项非常棘手的任务，需要随时应对被抽查检查，这就更需要一劳永逸的解决方案，那就是国密 HTTPS 加密自动化解决方案。

(3) 11 月 21 日，中国人民银行、国家发展改革委、工业和信息化部、金融监管总局、中国

(C) 2025 零信技术（深圳）有限公司

证监会、国家数据局、国家外汇局等七部门联合印发了《推动数字金融高质量发展行动方案》，要求所有金融机构都必须采用商用密码来保障金融数据安全和网络安全，这是要求银行官网、网银系统和银行业务系统必须实现国密 HTTPS 加密。

这对于所有金融机构来讲，也是一个非常棘手的任务，虽然金融机构早在 2018 年就已经开始国密改造，但是目前仍然只有一个银行官网实现了国密 HTTPS 加密，还有大量金融机构的官网甚至都还没有启用 HTTPS 加密。因为传统的国密 HTTPS 加密改造太难，只有零改造的国密 HTTPS 加密自动化解决方案才能真正解决金融系统国密 HTTPS 加密改造难题。

七、 小结

本期报告在 2025 元旦假期完成，零信技术的新年海报主题为：**2025 密.中国，密码保障甜蜜生活**。这个海报主题也是本季度报告的主题，因为只有普及应用商用密码才能真正保障我国网络空间安全，只有普及应用国密 SSL 证书实现国密 HTTPS 加密，才能保障我国网站系统安全，这是网络空间安全的基础安全保障，所以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，才会有小家的甜蜜生活。

为了国家的长治久安，密码人和网安人大家继续齐加油，2025，密·中国。

零信任安全研究院 和 零信浏览器 联合发布

2025 年 1 月 3 日于深圳

(C) 2025 零信技术（深圳）有限公司

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 199 篇(共 57 万 9 千多字)和英文 84 篇(10 万 9 千多单词)。

(C) 2025 零信技术（深圳）有限公司