中国 SSL 证书市场发展趋势分析简报-2024Q2

2024 年 7 月 1 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 2 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，特别是商密 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。同时继续发布全球十大 SSL 证书提供商的排名情况与分析，供国内 CA 及相关企业制定发展战略参考。

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 **2024 年 6 月 30 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 **7.4496** 亿张，比上一季度增加了 **6%**，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，可以看出 SSL 证书总数增长了 6%，但 DV SSL 证书却增长了 10%，说明 DV SSL 证书的比例仍然在持续增长，其占比由上一季度的 87.29%增长到 90.78%。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 2297 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 4532 万张，占比仅为 **6.08%**。所以，实际上，DV SSL 证书占比为 **93.87%**，连续 3 个季度保持这个高比例，这意味着 DV SSL 证书已经一统天下，非 DV SSL 证书仅占不到 **7%**！

	DV SSL证书	OV SSL证书	EV SSL证书
签发量	676,320,675	68,293,467	380,792
占比	90.78%	9.17%	0.05%
环比增长	10.29%	-23.23%	9.22%

表 1

全球 **7. 4496 亿**张有效证书中，排名前十六大 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 9.25%，首次超过 50%市场份额，第 2 位是 GoDaddy，保持上季度的第 2 位。谷歌由上季度的第 4 位上升到本季度第 3 位。

排名	公司名称	签发量	占比%	环比增长	上季度排名	公司类型	国别
1	Let's Encrypt	380,414,964	51.06%	9.25%	1	互联网软件	美国
2	GoDaddy	90,890,863	12.20%	26.68%	2	域名注册商	美国
3	谷歌	61,658,600	8.28%	12.49%	4	互联网公司	美国
4	亚马逊	57,839,692	7.76%	0.12%	3	云服务提供商	美国
5	DigiCert	44,856,325	6.02%	37.59%	6	CA机构	美国
6	Sectigo	33,479,945	4.49%	21.62%	7	CA机构	美国
7	Cloudflare	22,966,535	3.08%	-42.79%	5	CDN服务提供商	美国
8	微软	19,298,678	2.59%	-18.97%	8	云服务提供商	美国
9	ZeroSSL	14,399,089	1.93%	-18.58%	9	SSL证书提供商	奥地利
10	cPanel	6,171,036	0.83%	-40.07%	10	软件提供商	美国
11	IdenTrust	3,599,569	0.48%	-18.72%	11	CA机构	美国
12	思科	1,820,070	0.24%	13.57%	12	网络设备制造商	美国
13	GlobalSign	1,497,538	0.20%	1.83%	13	CA机构	日本
14	亚数信息	1,312,268	0.18%	21.58%	14	SSL证书提供商	中国
15	Actalis	817,015	0.11%	1.15%	15	CA机构	意大利
16	Entrust	569,075	0.08%	3.15%	16	CA机构	加拿大
	其他	3,371,601	0.45%	-57.93%			
	合计	**744,962,863**		**6.03%**			**2024Q2**

表 2

本期继续直接采用表格形式列出全球前 16 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 16 大中美国不仅占据前 8 大，而且共有 11 家，占比 69%，证书签发量占 97.05%。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。而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，也是拥有自己顶级根的 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 16 大 SSL 证书提供商的证书签发量排名和占比情况。

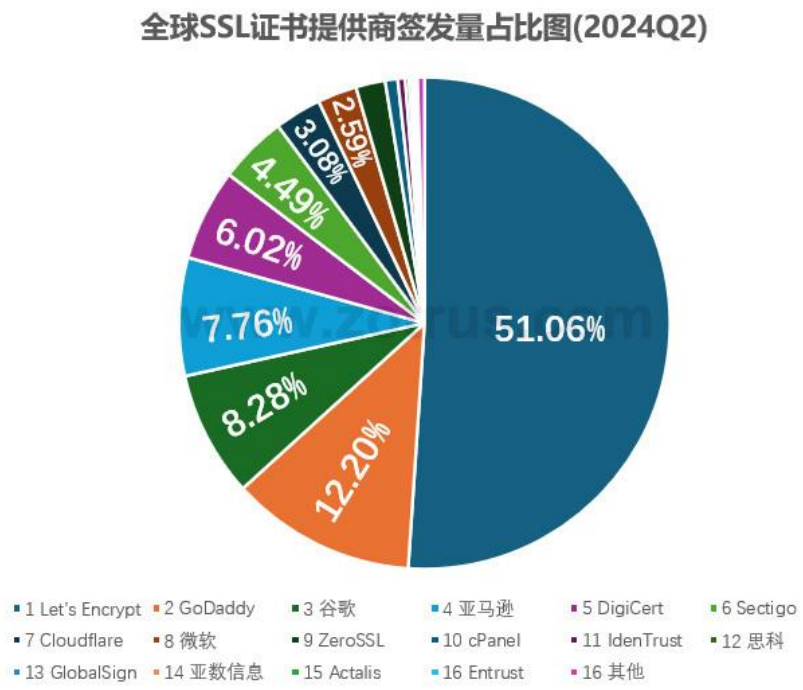

图 1

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，估计今年会落地。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，商密 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 **1768** 张，比上一季度增加了 **8.27%**，连续两个季度都在增长。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**，重庆市从上季度排名 20 位本季度上升到 15 位，河北省从上季度排名 22 位本季度上升到 18 位。

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	254	17.59%	14.37%	shanghai.gov.cn, sh.gov.cn	是	否		B
2	浙江省	181	-4.23%	10.24%	zj.gov.cn	是	否		B+
3	北京市	128	-1.54%	7.24%	beijing.gov.cn	是	否	有	B+
4	海南省	113	5.61%	6.39%	hainan.gov.cn	是	是		B+
5	广西壮族自治区	101	5.21%	5.71%	gxzf.gov.cn	否	否		
6	广东省	77	1.32%	4.36%	gd.gov.cn	否	否		
7	天津市	70	12.90%	3.96%	tj.gov.cn	是	否	有	A
8	宁夏回族自治区	69	11.29%	3.90%	nx.gov.cn	是	否		B+
9	云南省	62	-4.62%	3.51%	yn.gov.cn	是	否		B+
10	河南省	61	8.93%	3.45%	henan.gov.cn	是	否		B+
11	山东省	58	18.37%	3.28%	shandong.gov.cn, sd.gov.cn	否	否		
12	江西省	47	4.44%	2.66%	jiangxi.gov.cn	否	否		
13	甘肃省	46	12.20%	2.60%	gansu.gov.cn	是	否		B+
14	吉林省	45	12.50%	2.55%	jl.gov.cn	否	否	有	
15	重庆市	44	33.33%	2.49%	cq.gov.cn	是	否		
16	贵州省	40	11.11%	2.26%	guizhou.gov.cn	否	否		
17	黑龙江省	40	14.29%	2.26%	hlj.gov.cn	是	否	有	B+
18	河北省	39	25.81%	2.21%	hebei.gov.cn	否	否		
19	安徽省	38	0.00%	2.15%	ah.gov.cn	是	否	有	A
20	陕西省	35	-16.67%	1.98%	shaanxi.gov.cn	否	否		
21	湖南省	35	9.38%	1.98%	hunan.gov.cn	是	是		
22	新疆维吾尔自治区	33	0.00%	1.87%	xinjiang.gov.cn	是	有(登录页)		B
23	青海省	31	93.75%	1.75%	qinghai.gov.cn	否	否		
24	辽宁省	23	64.29%	1.30%	ln.gov.cn	是	否		B+
25	福建省	21	5.00%	1.19%	fujian.gov.cn, fj.gov.cn	是	否		B+
26	江苏省	19	0.00%	1.07%	jiangsu.gov.cn, js.gov.cn	否	否		
27	西藏自治区	18	50.00%	1.02%	xizang.gov.cn	否	否		
28	内蒙古自治区	15	0.00%	0.85%	nmg.gov.cn	是	否	有	A
29	山西省	11	0.00%	0.62%	shanxi.gov.cn	是	否		B+
30	湖北省	9	12.50%	0.51%	hubei.gov.cn	否	否		
31	四川省	5	25.00%	0.28%	sc.gov.cn	是	否		B+
	合计	**1768**	**8.27%**			**19**	**3**	**6**	

表 3

对于国密算法 SSL 证书的部署情况，本季度有新增，31 个省市自治区省级政府官网中部署了商密 SSL 证书的有两个省：湖南省和海南省。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 19 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，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 6 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和占比情况。

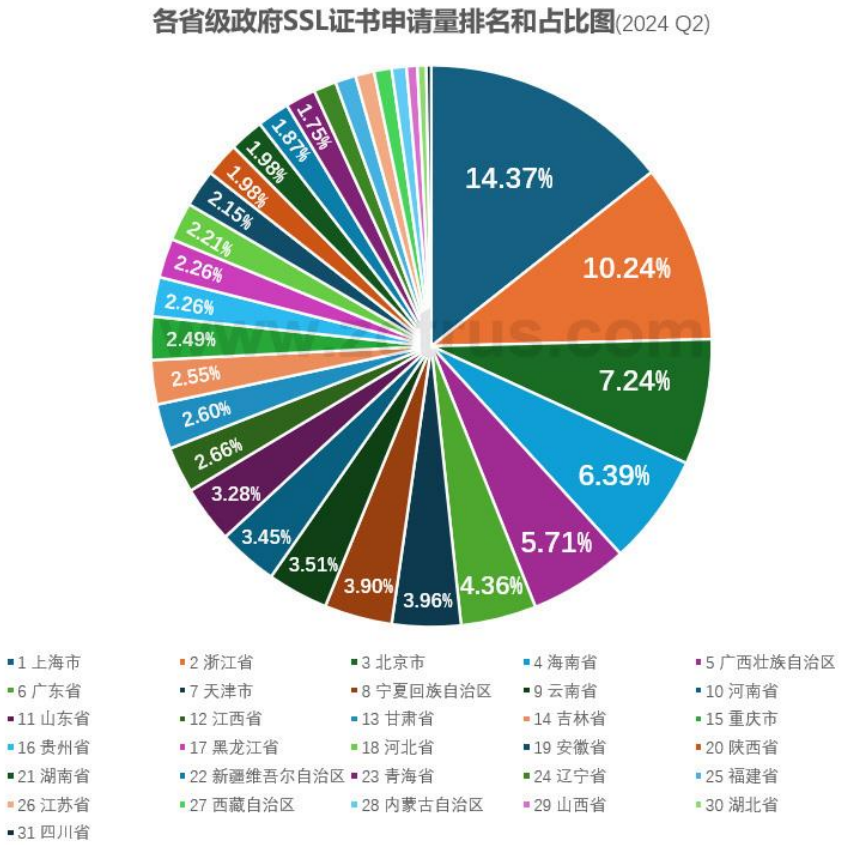

图 2

我们检索了 ***.gov.cn** 的 SSL 证书申请量为 **16905** 张，比上一季度增长了 **1.48%**，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 1768 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，政府用户仍然喜欢申请无需提供任何证明材料的 DV SSL 证书，占比 71%，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，这是因为中金认证的市场份额在快速上升中，国内 CA 机构可以做到不用麻烦用户提供证明材料而完成其身份认证，所以，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	11,975	4697	233
占比	70.84%	27.78%	1.38%
环比增长	-0.64%	7.51%	-1.27%

表 4

为政府网站*.gov.cn 签发这 16905 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：排名前三未变，沃通 CA 上升了 1 位。而美国 CA-DigiCert 下降了 14%，这是连续 4 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	6856	40.56%	-13.79%	美国	DigiCert (美国)
2	亚数信息	3089	18.27%	25.21%	中国	Sectigo/DigiCert (美国)
3	中金认证	1270	7.51%	3.34%	中国	CFCA (中国)
4	沃通CA	841	4.97%	15.21%	中国	Sectigo/DigiCert/Assecods (美国/波兰)
5	Let's Encrypt	761	4.50%	-12.93%	美国	ISRG (美国)
6	北京信查查	672	3.98%	19.79%	中国	Assecods/Sectigo (波兰/美国)
7	上海CA	659	3.90%	15.82%	中国	Assecods x UniTrust (中国)
8	数安时代	582	3.44%	4.86%	中国	Assecods/GDCA (波兰/中国)
9	GlobalSign	453	2.68%	3.42%	日本	GlobalSign (日本)
10	上海锐成	417	2.47%	54.44%	中国	Sectigo (美国)
11	Sectigo	410	2.43%	26.54%	美国	Sectigo (美国)
12	天威诚信	174	1.03%	4.19%	中国	Assecods (波兰)
13	ZeroSSL	152	0.90%	245.45%	奥地利	Sectigo (美国)
14	合肥网盾	121	0.72%	19.80%	中国	Sectigo/UniTrust (美国/中国)
15	新网数码	76	0.45%	46.15%	中国	UniTrust (中国)
16	北京新网	55	0.33%	44.74%	中国	Sectigo (美国)
17	腾讯云	53	0.31%	8.16%	中国	Sectigo (美国)
18	Assecods	36	0.21%	5.88%	波兰	Assecods (波兰)
19	其他	228	1.35%	47.10%		国外CA
合计		16,905		1.48%		2024Q2

表 5

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。

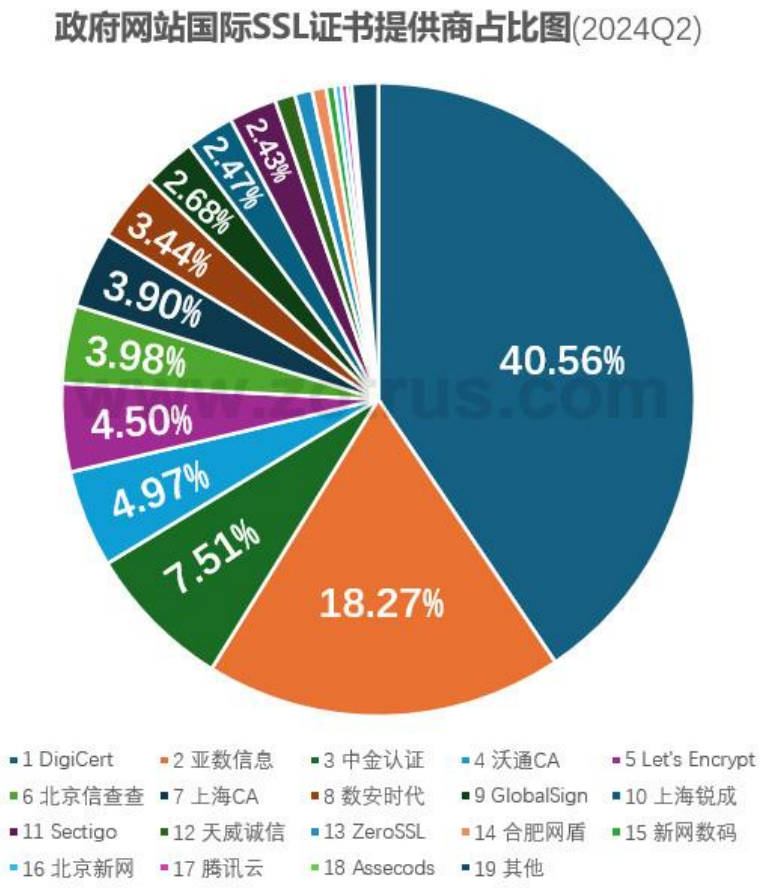

图 3

从本期开始，特别为拥有全球信任的 RSA 算法顶级根的国内 CA 机构-中金认证(CFCA)和上海 CA 单独列出其在政府市场的 SSL 证书的占比增长趋势图，从 2023Q2 有分析数据开始，已经连续 4 个季度增长，分别从 2023Q2 的占比 5.83%、2023Q3 的 6.29%、2023Q4 的 7.19%、2024Q1 的 10.78%到本季度的 11.41%。这说明政府用户在选购 SSL 证书时已经开始重视从拥有全球信任的顶级根的国内 CA 采购，以确保合规和供应安全。但是，即使 RSA 算法 SSL 证书是我国 CA 自己的顶级根证书签发，是否信任这些 RSA 算法根证书还是人家说了算，仍然有安全风险，普及自己说了算的商密 SSL 证书应用才是唯一安全上策。

图 4

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 **16905** 张，而台湾省本季度增长了 136%，第一次超过了大陆所有政府网站的证书申请量的总和。本期数据显示澳门特区都有小幅下降。

	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	16,905	1.48%	*.gov.cn	是	否	有	B+
中国台湾省	29,269	135.51%	*.gov.tw	是	否		B+
中国香港特别行政区	2,827	45.80%	*.gov.hk	是	否		B+
中国澳门特别行政区	454	-2.58%	*.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 19 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 19 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 10 家是商业公司。

而这 19 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 16 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，本季度新增两家-GeoSSL(未查到中文公司名称)和上海环度进入前 19 位。

这 19 家国际 SSL 证书提供商签发的有效证书数合计为 **146.3781** 万张，比上一季度增长了

24.66%，对比全球数据增加了 **6%**，说明国内 SSL 证书提供商的增长幅度高于全球市场，这 19 家的总和在全球 SSL 证书提供商中排名第 **14** 位。本季度最大的亮点是零信证签从上季度排名第 9 位一跃成为第 3 位，证书签发量增长 387%，这是由于零信国密 HTTPS 加密自动化网关本季度已经在全国各地政府单位、银行和高校部署试用和测试，不仅测试能自动化签发 90 天的 DV/OV/EV SSL 证书，并且正在测试每天自动化更新证书，以应对即将落地的 90 天证书政策，并且可以应对将来可能的继续缩短 SSL 证书有效期的情况，哪怕是一天有效期。

全球排名前 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，也只有自动化才能降低 HTTPS 部署成本和杜绝遗忘续期的风险，只有自动化部署才能提升 HTTPS 加密服务的安全性和敏捷性，轻松帮助用户实现大规模的 SSL 证书部署，零改造完成商密 HTTPS 加密改造，满足用户商密合规、等保合规、密保合规、关保合规和全球信任等网络与通信安全及应用和数据安全的合规要求，快速实现所有互联网政务应用的商密 HTTPS 加密安全连接。

排名	公司简称	签发量	增长%	占比%	根CA (国别)
1	亚数信息	1,312,315	21.72%	89.65%	Sectigo/DigiCert (美国)
2	上海锐成	52,663	69.35%	3.60%	Sectigo (美国)
3	零信证签	20,294	387.02%	1.39%	Sectigo/UniTrust (美国/中国)
4	北京信查查	18,044	13.82%	1.23%	Assecods/Sectigo (波兰/美国)
5	沃通CA	15,168	35.31%	1.04%	Sectigo/DigiCert/Assecods (美国/波兰)
6	合肥网盾	13,102	74.81%	0.90%	Sectigo/UniTrust (美国/中国)
7	中金认证	6,680	3.68%	0.46%	CFCA (中国)
8	上海CA	5,618	16.87%	0.38%	UniTrust (中国)
9	腾讯云	5,209	8.34%	0.36%	Sectigo (美国)
10	天威诚信	3,304	18.81%	0.23%	Assecods (波兰)
11	阿里云	2,191	63.75%	0.15%	GlobalSign (日本)
12	百度云	1,433	44.16%	0.10%	Sectigo (美国)
13	数安时代	1,352	6.79%	0.09%	Assecods/GDCA (波兰/中国)
14	北京新网	1,325	13.25%	0.09%	Sectigo (美国)
15	新网数码	1,216	58.33%	0.08%	UniTrust (中国)
16	浙江葫芦娃	1,127	37.27%	0.08%	Sectigo (美国)
17	GeoSSL	686		0.05%	Sectigo (美国)
18	厦门纳网	440	116.75%	0.03%	Sectigo (美国)
19	上海环度	350		0.02%	UniTrust (中国)
20	其他	1,264	163.33%	0.09%	
合计		**1,463,781**	**24.66%**		**2024Q2**

表 7

本期合计统计 **1,463,781** 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 **98.10**%，这个比例比全球市场的 DV SSL 证书的占比 93%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，从这个方面也印证了第二部分的国内 CA 的市场份额持续四个季度都在增长的原因。

	DV SSL证书	OV SSL证书	EV SSL证书
数量	1,436,025	26,360	1290
占比	98.10%	1.81%	0.09%

表 8

四、 我国商密 SSL 证书提供商的统计数据分析

本期发布的商密 SSL 证书数据来自零信国密证书透明日志系统(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，本次报告的商密 SSL 证书数据仅供参考。合计 **23248** 张，比上一季度增长了 **360%**，这是由于零信网关的大范围测试和试用而自动化签发了大量的商密 SSL 证书。商密 SSL 证书连续 7 个季度持续增长，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，不仅有省级政府网站实现了国密 HTTPS 加密(如湖南省和海南省)，并且有多个地级市政务服务网站也已经实现国密 HTTPS 加密。

五、 本季度与 SSL 证书市场相关的大事解读

本季度发生了两件与 SSL 证书市场相关的大事，第一件大事是我国四部委联合发布了《互联网政务应用安全管理规定》(以下简称《规定》)，第二件大事是谷歌浏览器宣布从 11 月 1 日起不再信任加拿大 CA-Entrust 签发的 SSL 证书。

第一件大事绝对是一件 SSL 证书市场的大利好，同时也是保障我国互联网更加安全的重要措施。这是由网信办、中央编办、工信部和公安部联合发布的，今天(7 月 1 日)正式施行，是为了保障互联网政务应用安全稳定运行和数据安全。

具体与 SSL 证书相关的有两点：一是所有政府网站包括所有关键信息基础设施网站都必须采用商密 HTTPS 加密方式实现安全连接；二是所有政府网站如果采用的 CDN 服务的话，则要求 CDN 服务必须支持商密 HTTPS 加密。如果违反或者未能正确履行《规定》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。这就是要相关单位必须马上行动起来去落实，以满足《规定》的要求。而如何行动，就需要寻找合适的解决方案，是采用传统的购买 SSL 证书去每台服务器人工部署，每年一次或者 5 次，还是采用自动化方式一劳永逸的，这个一定要看准方向，不能花了钱并没有真正解决

问题。

而对于 CA 机构和 SSL 证书提供商，则应抓住此巨大的机遇，为互联网政务应用提供相应的产品和解决方案，这个核心产品当然是 SSL 证书，但是如何为政府用户提供 SSL 证书，是采用传统的仅销售 SSL 证书还是为政府用户提供 SSL 证书自动化管理服务，这个一定要看准方向，走对技术路线才能抓住商机。

第二件大事绝对是一个对我国 CA 包括 SSL 证书提供商和我国 SSL 证书用户都有巨大影响的事件，必须高度重视。对于 CA 机构来讲，头上永远悬着一把利剑，不知道哪一天就会被谷歌这把利剑刺伤。所以，不仅必须严格地按照国际标准签发国际 SSL 证书，而且必须有如果这边利剑落下来的应对预案，必须有多通道为用户签发国际 SSL 证书的能力。

而对于 SSL 证书用户来讲，传统的从 CA 机构申请 SSL 证书去人工部署方案不仅费时费力，而且不保险，说不定哪一天你使用的 SSL 证书签发机构的根就不受信任了，需要你重新申请证书和重新部署证书，这将是一个巨大的工作负担，这事对于 SSL 证书用户来讲真的非常无辜，但是没有办法。所以，最明智的做法是采用自动化方案，要求自动化证书管理服务提供商保证无论发生什么情况都能自动化实现 HTTPS 加密，也就是自动化方案不绑定某个 CA 机构，而是可以自动化切换证书签发通道，确保无论发生任何情况都无需重新申请和部署 SSL 证书，这才是一劳永逸的解决方案，这个方案也只有自动化方案才能做到。

六、小结

四部委发布的《互联网政务应用安全管理规定》今天(7 月 1 日)正式施行，这是我国 SSL 证书市场将获得更加快速增长的方向标，并必将进一步提升我国互联网政务应用安全稳定运行水平和数据安全水平。当然，这也是密码业界和网络安全业界的一个大利好，希望大家能抓住这个发展机遇。

2024 年是“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。

零信任安全研究院和**零信浏览器** 联合发布

2024 年 7 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 171 篇(共 47 万多字)和英文 68 篇(8 万 4 千多单词)。