中国 SSL 证书市场发展趋势分析简报-2024Q1

2024 年 4 月 1 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 2024 年第一季度分析报告，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。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 3 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 **7.0258** 亿张，比上一季度增加了 **3.84%**，首次突破 **7** 亿张。从本期开始不再发布从 2013 年以来累计签发了多少张 SSL 证书的数据，因为 90%以上的 SSL 证书都是 90 天有效期，每个域名每年重复签发 5 次，这些已经过期的 SSL 证书的数量已经没有任何参考价值。

全球有效的 SSL 证书总数为 **7.0258** 亿张，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 3.84%，但 DV SSL 证书却增长了 6.01%，说明 DV SSL 证书的比例仍然在持续增长。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 4014 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 4882 万张，占比仅为 **6.95%**。所以，实际上，DV SSL 证书占比为 **93%**，连续两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	613,243,766	88,956,179	348,660
占比	87.29%	12.66%	0.05%
环比增长	6.01%	-8.84%	1.66%

表 1

全球 **7.0258 亿**张有效证书中，排名前十七大 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%，但稍微低于 50%市场份额一点点，第 2 位是 GoDaddy，从上上季度的第 7 位上升到上季度的 5 位，这个季度快速上升到第 2 位，这是火箭式的快速上升。谷歌在上上季度的第 3 位上升到上季度的第 2 位，本季度下降到第 4 位。Cloudflare 从上上季度的第二位下跌到上季度的第 4 位，本季度继续下跌到第 5 位。这些变化的深层原因在第五部分深入分析。

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	348,213,161	49.56%	12.02%	1	互联网软件	美国
2	GoDaddy	71,749,868	10.21%	48.12%	5	域名注册商	美国
3	亚马逊	57,772,431	8.22%	6.18%	3	云服务提供商	美国
4	谷歌	54,814,713	7.80%	-4.45%	2	互联网公司	美国
5	Cloudflare	40,143,918	5.71%	-20.84%	4	CDN服务提供商	美国
6	DigiCert	32,600,295	4.64%	-1.42%	7	CA机构	美国
7	Sectigo	27,527,847	3.92%	-37.42%	6	CA机构	美国
8	微软	23,817,165	3.39%	6.24%	9	云服务提供商	美国
9	ZeroSSL	17,686,024	2.52%	-28.96%	8	SSL证书提供商	奥地利
10	cPanel	10,296,674	1.47%	-16.06%	10	软件提供商	美国
11	IdenTrust	4,428,484	0.63%			CA机构	美国
12	思科	1,602,529	0.23%			网络设备制造商	美国
13	GlobalSign	1,470,674	0.21%			CA机构	日本
14	亚数信息	1,079,341	0.15%			SSL证书提供商	中国
15	Actalis	807,687	0.11%			CA机构	意大利
16	Entrust	551,711	0.08%			CA机构	加拿大
17	Gandi	419,591	0.06%			SSL证书提供商	法国
18	其他	7,595,405	1.08%				
	合计	**702,577,518**		**3.84%**			**2024Q1**

表 2

从本期开始直接采用表格形式列出全球前 17 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 17 大中美国不仅占据前 8 大，而且共有 11 家，占比 65%。

我国有一家，但是并不是顶级根 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。

从本期开始，如下图 1 所示，用圆饼图直观展示全球前 17 大 SSL 证书提供商的证书签发量排名和占比情况。

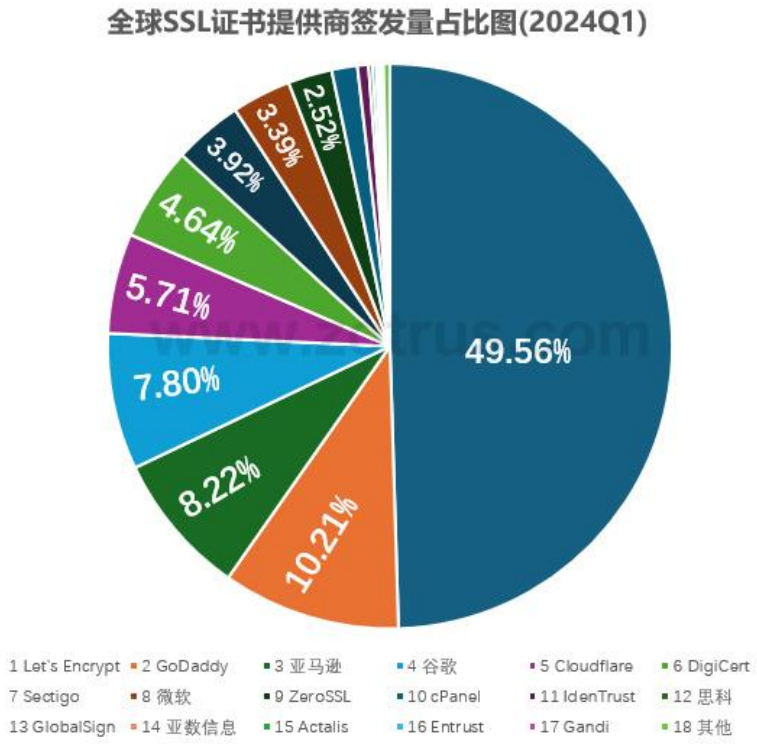

图 1

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，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 **1633** 张，比上一季度增加了 **5.02%**，连续两个季度都在增长。其中，上海市上升了一位，升到第 1 名。云南省上升了 5 位，黑龙江省上升最多，升了 7 位，这个可能与“尔滨”的火热有关。排名前 5 位的是**上海市、浙江省、北京市、海南省、广西壮族自治区。**

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	216	10.77%	13.23%	shanghai.gov.cn, sh.gov.cn	是	否		B
2	浙江省	189	-5.03%	11.57%	zj.gov.cn	是	否		B+
3	北京市	130	-0.76%	7.96%	beijing.gov.cn	是	否	有	B+
4	海南省	107	5.94%	6.55%	hainan.gov.cn	是	否		B+
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		B+
8	天津市	62	1.64%	3.80%	tj.gov.cn	是	否	有	A
9	宁夏回族自治区	62	-1.59%	3.80%	nx.gov.cn	是	否		B+
10	河南省	56	7.69%	3.43%	henan.gov.cn	是	否		B+
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		B+
15	吉林省	40	-4.76%	2.45%	jl.gov.cn	否	否	有	
16	安徽省	38	8.57%	2.33%	ah.gov.cn	是	否	有	A
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	有	B+
19	新疆维吾尔自治区	33	50.00%	2.02%	xinjiang.gov.cn	是	有(登录页)		B
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		B+
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	有	A
27	辽宁省	14	0.00%	0.86%	ln.gov.cn	是	否		B+
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		B+
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		B+
	合计	1633	5.02%			18	2	6	

表 3

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。

从本期开始，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。

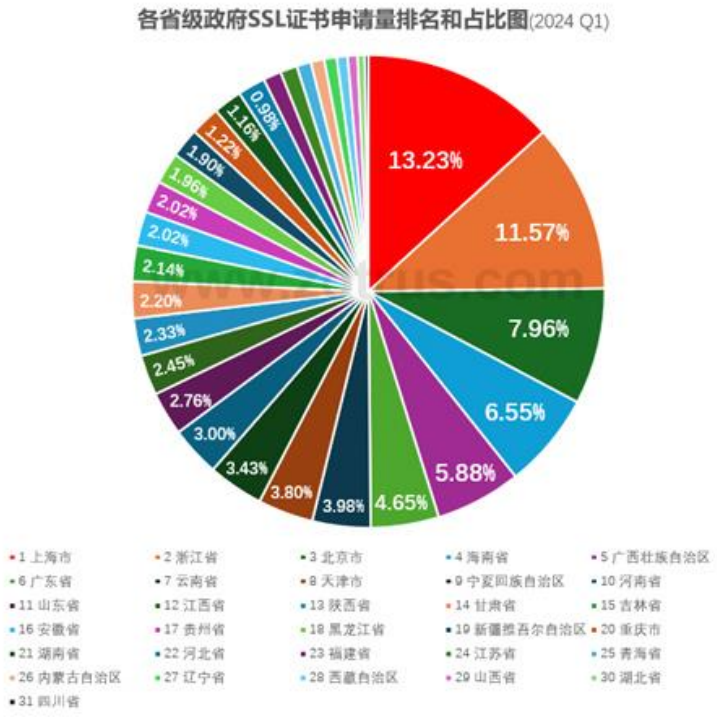

图 2

我们检索了 ***.gov.cn** 的 SSL 证书申请量为 **16658** 张，比上一季度减少了 **1.53%**，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 1633 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 72%，比上期有所下降。而需要提供身份认证证明材料的 OV SSL 证书和 EV SSL 证书都有所上升，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/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。

	DV SSL证书	OV SSL证书	EV SSL证书
签发量	12,052	4,369	236
占比	72.35%	26.23%	1.42%
环比增长	-6.56%	15.16%	4.43%

表 4

为政府网站*.gov.cn 签发这 16658 张 SSL 证书的 SSL 证书提供商前 19 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：中金认证从上季度的第 5 位上升到第 3 位，上海 CA 从上季度的第 8 位上升到第 6 位，值得祝贺！

排名	公司简称	证书数	占比	增长%	国别	根CA (国别)
1	DigiCert	7,953	47.74%	-8.90%	美国	DigiCert (美国)
2	亚数信息	2,467	14.81%	-5.88%	中国	Sectigo/DigiCert (美国)
3	中金认证	1,229	7.38%	73.83%	中国	CFCA (中国)
4	Let's Encrypt	874	5.25%	0.34%	美国	ISRG (美国)
5	沃通CA	730	4.38%	-0.68%	中国	Sectigo/DigiCert/Assecods (美国/波兰)
6	上海CA	569	3.42%	11.57%	中国	Assecods x UniTrust (中国)
7	北京信查查	561	3.37%	6.86%	中国	Assecods/Sectigo (波兰/美国)
8	数安时代	555	3.33%	-9.02%	中国	Assecods + GDCA (波兰 + 中国)
9	GlobalSign	438	2.63%	1.86%	日本	GlobalSign (日本)
10	Sectigo	324	1.95%	-7.16%	美国	Sectigo (美国)
11	上海锐成	270	1.62%	18.94%	中国	Sectigo (美国)
12	天威诚信	167	1.00%	12.84%	中国	Assecods (波兰)
13	合肥网盾	101	0.61%	4.12%	中国	Sectigo (美国)
14	新网数码	52	0.31%		中国	UniTrust (中国)
15	腾讯云	49	0.29%	-10.91%	中国	Sectigo (美国)
16	Cloudflare	48	0.29%	-2.04%	美国	DigiCert (美国)
17	ZeroSSL	44	0.26%	15.79%	奥地利	Sectigo (美国)
18	北京新网	38	0.23%	-9.52%	中国	Sectigo (美国)
19	Assecods	34	0.20%	13.33%	波兰	Assecods (波兰)
20	其他	155	0.93%	8.39%		国外CA
合计		**16,658**				2024Q1

表 5

从本期开始，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。

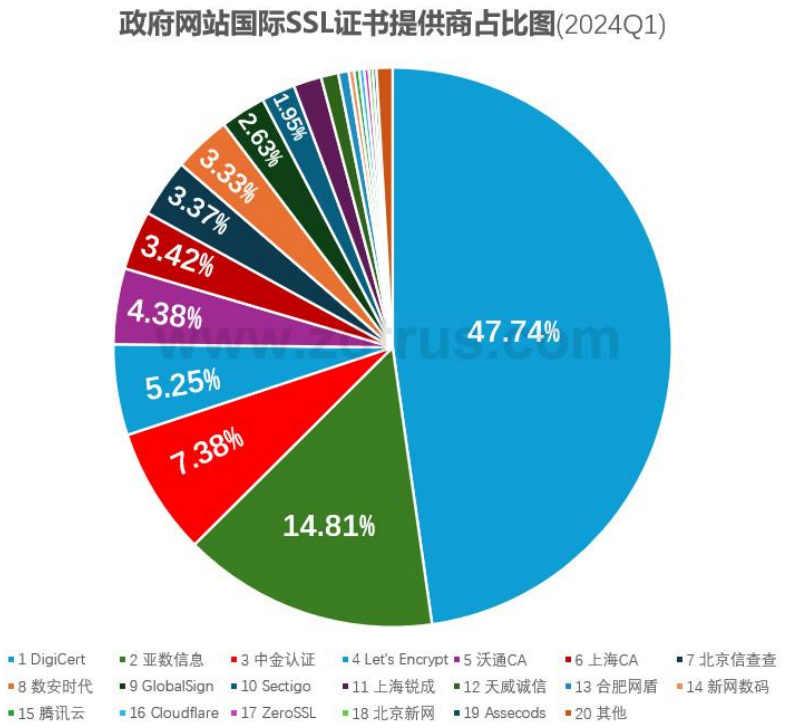

图 3

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% 到 2024Q1 的 10.78%，增长幅度高达 185%。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 **16658** 张，连续四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。本期数据显示大陆、台湾省和香港特区都有小幅下降。

	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	**16658**	-1.53%	*.gov.cn	是	否	有	B+
中国台湾省	**12428**	-0.85%	*.gov.tw	是	否		B+
中国香港特别行政区	**1939**	-4.15%	*.gov.hk	是	否		B+
中国澳门特别行政区	**466**	6.64%	*.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 8 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 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，本季度新增一家-厦门纳网进入前 19 位。

这 19 家国际 SSL 证书提供商签发的有效证书数合计为 **117.4241** 万张，比上一季度减少了 **7.85%**，对比全球数据增加了 **3.84%**，国内 SSL 证书提供商的市场份额连续四个季度在下降，

这 19 家的总和在全球 SSL 证书提供商中排名第 **14** 位。而全球排名前 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，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。

排名	公司简称	证书签发量	增长%	占比%	根CA (国别)	上季度排名
1	亚数信息	1,078,142	-9.98%	91.82%	Sectigo/DigiCert (美国)	1
2	上海锐成	31,098	55.59%	2.65%	Sectigo (美国)	2
3	北京信查查	15,853	9.66%	1.35%	Assecods/Sectigo (波兰/美国)	3
4	沃通CA	11,210	7.06%	0.95%	Sectigo/DigiCert/Assecods (美国/波兰)	4
5	合肥网盾	7,495	31.40%	0.64%	Sectigo (美国)	5
6	中金认证	6,443	58.85%	0.55%	CFCA (中国)	**8**
7	腾讯云	4,808	-3.69%	0.41%	Sectigo (美国)	6
8	上海CA	4,807	10.51%	0.41%	Assecods x UniTrust (中国)	7
9	零信证签	4,167	10.65%	0.35%	Sectigo (美国)	9
10	天威诚信	2,781	11.91%	0.24%	Assecods (波兰)	10
11	阿里云	1,338	39.23%	0.11%	GlobalSign (日本)	**14**
12	数安时代	1,266	-2.69%	0.11%	Assecods + GDCA (波兰 + 中国)	11
13	北京新网	1,170	-7.87%	0.10%	Sectigo (美国)	12
14	百度云	994	1.33%	0.08%	Sectigo (美国)	13
15	浙江葫芦娃	821	0.37%	0.07%	Sectigo (美国)	15
16	新网数码	768	59.34%	0.07%	Assecods x UniTrust (中国)	16
17	北京中万	208	0.48%	0.02%	Sectigo (美国)	17
18	厦门纳网	203		0.02%	Sectigo (美国)	
19	深圳CA	189	-6.44%	0.02%	Assecods (波兰)	18
20	其他	480		0.04%		
合计		**1,174,241**	**-7.85%**		2024Q1	

表 7

本期值得注意的有三个数据：

(1) 中金认证从上季度的第 8 位上升到了第 6 位，并且是唯一一个不销售仅验证域名的低端 DV SSL 证书的 CA 机构，能取得这样的成绩只能说明用户已经认可国内 CA 机构签发的国际 SSL 证书。

(2) 阿里云已经发力 SSL 证书市场，从上季度的第 14 位上升到了第 11 位，值得关注。

(3) 排名第一位的亚数信息从 2023 年第 1 季度开始到本季度已经连续 5 个季度在下降，下降幅度最高的有 39.47%，最低也有 3.21%。

从本期开始，增加这些本土国际 SSL 证书提供商所签发的 SSL 证书的类型统计数据，这样可以让相关方了解我国用户对 SSL 证书类型的选择取向。本期合计统计 **1,174,241** 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 **97.94%**，这个比例比全球市场的 DV SSL 证书的占比 93%高出一点点，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	1,150,110	22,935	1,196
占比	97.94%	1.96%	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(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 **6448** 张，比上一季度增长了 **48.95%**，连续 6 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)，并且有多个地级市政务服务网站也已经实现国密 HTTPS 加密(如宝鸡市)。

本季度新增一家 CA 机构-贵州 CA 签发的国密 SSL 证书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 3 家 CA 机构签发的国密 SSL 证书支持国密证书透明标准草案，本报告将在下个季度开始像国际 SSL 证书一样列表排名各个国密 SSL 证书提供商签发的国密 SSL 证书，以帮助用户在选购国密 SSL 证书时优先选择支持国密证书透明的国密 SSL 证书提供商，从而保障用户自身的合法权益和网站安全。

零信浏览器已经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，各家国密 CA 机构还有三个月时间去完成升级 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，对没有在国密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、全球十大 SSL 证书提供商排名变化分析与启示

本期继续发布全球前十大 SSL 证书提供商的排名变化情况，从中可以拓展我国 SSL 证书提供商的发展思路，这个很有价值。如下表 9 所示，Let's Encrypt 仍然是稳居第一位，并且比上一季度增长了 12%，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，也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位 GoDaddy 的 4.85 倍，比其他 9 位的总和还要多。

本期最耀眼的是 GoDaddy (红色曲线)，从 2023Q1 排名第 9 位，只用了一年时间，一跃到了现在的第 2 位，其原因是 GoDaddy 是一个老牌域名注册商，拥有互联网用户来源入口，这些用户的域名在 GoDaddy 注册，只要 GoDaddy 为用户提供一站式建站服务，自动化提供网站所需的 SSL 证书，用户不会再去找其他家申请 SSL 证书了。这绝对是国内域名注册商好好学习的榜样，不能守着金山没饭吃，必须尽快为用户提供一站式建站服务和提供 SSL 证书自动化服务，当然必须是定制自己品牌的 SSL 中级根证书，否则统计数据还是人家的。而 GoDaddy 直接拥有自己的全球信任的顶级根证书，这在我国很难做到，只能通过定制 SSL 中级根证书来快速达到一样的效果。

	2023 Q1排名	2023 Q2排名	2023 Q3排名	2023 Q4排名	2024 Q1排名
1	Let's Encrypt	Let's Encrypt	Let's Encrypt	Let's Encrypt	Let's Encrypt
2	Cloudflare	Cloudflare	Cloudflare	谷歌	GoDaddy
3	亚马逊	谷歌	谷歌	亚马逊	亚马逊
4	谷歌	亚马逊	亚马逊	Cloudflare	谷歌
5	Sectigo	Sectigo	Sectigo	GoDaddy	Cloudflare
6	DigiCert	DigiCert	DigiCert	Sectigo	DigiCert
7	微软	微软	GoDaddy	DigiCert	Sectigo
8	cPanel	cPanel	微软	ZeroSSL	微软
9	GoDaddy	GoDaddy	ZeroSSL	微软	ZeroSSL
10	ZeroSSL	ZeroSSL	cPanel	cPanel	cPanel

表 9

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 2023Q1 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。但是为何本季度一下子下降到第 4 位呢？最大的可能是 GoDaddy 用户原先是使用谷歌的自动化证书服务，但是一旦 GoDaddy 也提供了自动化证书服务，则用户就直接用 GoDaddy 的自动化证书服务了。从这一点可以看出，互联网巨头如果不拥有用户来源入口，也是有其发展局限的。

第三个值得关注的是 Cloudflare，从上上季度的第二位下跌到上季度的第 4 位，本季度下跌到第 5 位，只是因为没有自己的顶级根，定制的中级根证书可能受根 CA 的约束而从上上季度开始直接为用户自动化提供 LE 和谷歌的 SSL 证书，导致自己品牌的 SSL 证书市场份额持续下降。

第四个值得关注的是 DigiCert 和 Sectigo，全球前两大 CA 机构理应排名第一和第二，本季度分别排名第 6 个和第 7 位，Sectigo 下降了一位，可能与该公司最近经常在周末升级系统而无法签发证书有关。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呢？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，预计还会继续下滑。这是 CA 机构的劣势，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。

国内 CA 机构有国外 CA 机构不一样的优势就是国密改造需要国密 SSL 证书，国内 CA 机构可以通过抓住国密改造的机会实现突破，因为用户同时需要国密 SSL 证书和国际 SSL 证书，实现双算法双 SSL 证书部署。每个能签发国密 SSL 证书的 CA 机构都应该能同时签发自己品牌的国际 SSL 证书，而不是代理其他品牌的国际 SSL 证书，这样就可以通过国密 SSL 证书的刚需来带动起其国际 SSL 证书市场份额的提升。而要实现快速提升，唯有自动化，唯有普及应用国密 HTTPS 加密自动化网关才能让用户零改造实现双 SSL 证书的自动化供给和自动化部署。

六、小结

本期报告有两个方面的改进，一是更多地采用了图表，让用户对各种数据一目了然。二是重点分析了国际 SSL 证书的发展趋势对我国相关厂商的发展战略参考，并且重点关注了用户

对国内 CA 机构签发的国际 SSL 证书的增长数据，以帮助用户在选购国际 SSL 证书时能更多关注国内 CA 机构，以满足政府用户对数据出境安全风险管理的实际需要。当然，我国 SSL 证书发展的最终市场机会是国密 SSL 证书，只有相关产业各界都积极推动国密 SSL 证书自动化的应用，真正解决用户在使用国密 SSL 证书中的痛点，才能让用户积极选用国密 SSL 证书，真正普及应用国密 SSL 证书来保障我国网空安全。

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。

零信技术零信任安全研究院

2024 年 4 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 156 篇(共 41 万多字)和英文 61 篇(7 万多单词)。