中国 SSL 证书市场发展趋势分析简报-2023Q3

零信任安全研究院全球独家发布

(2023 年 10 月 3 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 年第三季度分析报告，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，同时增加了我国前 20 大银行的 SSL 证书签发数据，这两个重要领域的 SSL 证书签发数据非常有参考价值，因为从俄乌冲突发生后第 10 天开始美国 CA 就开始吊销了三千多张俄罗斯政府网站和银行网站的 SSL 证书，从而导致这些重要的网站系统都无法正常访问，不仅严重影响了老百姓上网办事，更可怕的是严重动摇了民心。以史为鉴，可知兴替。零信任安全研究院特在这个举国欢庆的日子里发布这些有重要参考价值的数据，希望这些数据和建议能为相关政府部门和商业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 10 月 1 日**，已经在国际证书透明日志系统记录的全球 SSL 证书总数已经突破 **100 亿**张，为 **10679979979** 张(**106** 亿多)，其中未过期的全球信任的 SSL 证书有 **6.1436** 亿张，比上一季度减少了 **5.77%**，略有下降。

全球 **6.1436 亿**张有效证书中，只验证域名的 DV SSL 证书有 **5.1445 亿**张，比第一季度减少了 **5.31%**，占比 **83.74%**，增加了 0.41。验证网站身份的 OV SSL 证书有 **9954 万**张，比上一季度减少了 **7.99%**，占比 **16.20%**，下降了 0.39。扩展验证网站身份的 EV SSL 证书 **34.513 35.996 万张**，比上一季度减少了 **4.12%**，占比 **0.056%**，下降了 **30%**。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，可以理解为这是错误签发的 OV SSL 证书，实际上是 DV SSL 证书！所以，OV SSL 证书的数据已经不能真实反映真正的 OV SSL 证书的占比，仅供参考。

也正是由于大量的 CDN 用 SSL 证书和物联网用 SSL 证书的 O 字段信息的不准确，再加

上少数签发给政府网站的 OV SSL 证书的 O 字段信息居然是公司名称，这使得我们确信以前根据 OV SSL 证书和 EV SSL 证书的数据来统计各国的 SSL 证书申请情况并排名已经失去了可比性，所以本期继续不再做国别排名，本期将重点分析我国网站所部署的 SSL 证书相关签发数据，这个对我国普及 SSL 证书应用更有现实意义。

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 位是 Let's Encrypt (2.9233 亿张)(比上一季度减少了 11.39%)、第 2 位是 Cloudflare (5538 万张)(减少)、第 3 位是谷歌 (5247 万张)(减少)、第 4 位是亚马逊 (5030 万张)(减少)、第 5 位是 Sectigo (4249 万张)(增加)、第 6 位是 DigiCert (3138 万张)(减少)、第 7 位是 GoDaddy (2579 万)(增加)、第 8 位是微软 (2262 万张)(减少)、第 9 位是 ZeroSSL (1358 万张)(增加)、第 10 位是 cPanel (1719 万张)(减少)。对比上一季度的数据，前 5 位中的前 4 位签发数量都有一定比例的减少，只有第 5 位的 Sectigo 有增加；而增长最快的是 GoDaddy，增加了 216%，从 9 位上升到第 7 位；下跌最多的是 cPanel，从第 8 名下降到第 10 位，这说明有自己的顶级根的 CA 还是有核心竞争力的。

全球排名前十的 SSL 证书提供商中，只有两家是传统的 CA 机构：Sectigo 和 DigiCert，其他家都是互联网和云服务提供商，这个非常值得我国的互联网和云服务提供商学习。因为用户需要的是网站支持 https 加密，而不是 SSL 证书！如果用户能从云服务提供商那里直接获得网站 https 加密服务，就不会再去 CA 申请 SSL 证书了，这也非常值得 CA 机构深思应该如何应对这个市场变化。Sectigo 市场份额有所上升的原因是提出了自动化证书管理的解决方案，这也是值得我国 CA 机构学习的。如果 CA 机构仍然是采用传统的手工申请 SSL 证书方式来销售 SSL 证书，则一定会被能提供自动化部署 SSL 证书的服务提供商超越，市场份额会重新洗牌！

再深度分析这 8 家互联网和云服务提供商签发的 SSL 证书发现，这高达 86%的 SSL 证书基本上都是免费的 90 天 DV SSL 证书，再加上 Sectigo 提供的 90 天免费证书，估计占比已经高达 90%，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 90%就是 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 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 **1435** 张，比上一季度减少了 **17.34%**，可能是有些省市自治区申请了通配证书，为了密钥安全，强烈不建议为所有网站共用一张通配证书。其中，海南省上升到第 5 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。河南省上升了 4 位，可能与今年 8 月份在河南省召开商用密码大会有关，进一步推动了河南省政务网站的 HTTPS 加密实施。其他排名上升还有陕西省、山东省、青海省等，排名前 5 位的是**浙江省、上海市、北京市、广西壮族自治区、海南省。**

排名	省市自治区	数量	检索域名	默认https	部署国密	WAF防护	安全评级
1	浙江省	209	zj.gov.cn	是	否		B+
2	上海市	175	shanghai.gov.cn, sh.gov.cn	是	否		B
3	北京市	115	beijing.gov.cn	是	否	有	B+
4	广西壮族自治区	92	gxzf.gov.cn	否	否		
5	海南省	82	hainan.gov.cn	是	否		B+
6	广东省	73	gd.gov.cn	否	否		
7	宁夏回族自治区	63	nx.gov.cn	是	否		B+
8	天津市	57	tj.gov.cn	是	否	有	A
9	河南省	45	henan.gov.cn	是	否		B+
10	江西省	44	jiangxi.gov.cn	否	否		
11	重庆市	42	cq.gov.cn	是	否		
12	陕西省	40	shaanxi.gov.cn	否	否		
13	吉林省	38	jl.gov.cn	否	否	有	
14	云南省	38	yn.gov.cn	是	否		B+
15	山东省	37	shandong.gov.cn, sd.gov.cn	否	否		
16	甘肃省	34	gansu.gov.cn	是	否		B+
17	贵州省	31	guizhou.gov.cn	否	否		
18	安徽省	31	ah.gov.cn	是	否	有	A
19	湖南省	27	hunan.gov.cn	否	有		
20	河北省	21	hebei.gov.cn	否	否		
21	福建省	20	fujian.gov.cn, fj.gov.cn	是	否		B+
22	青海省	18	qinghai.gov.cn	否	否		
23	江苏省	15	jiangsu.gov.cn, js.gov.cn	否	否		
24	辽宁省	15	ln.gov.cn	是	否		B+
25	黑龙江省	14	hlj.gov.cn	是	否	有	A
26	新疆维吾尔自治区	13	xinjiang.gov.cn	否	有		
27	山西省	13	shanxi.gov.cn	是	否		B+
28	内蒙古自治区	13	nmg.gov.cn	是	否	有	A
29	西藏自治区	10	xizang.gov.cn	否	否		
30	湖北省	7	hubei.gov.cn	否	否		
31	四川省	3	sc.gov.cn	是	否		B+
	合计	1435		17	2	6	

表 1

对于国密算法 SSL 证书的部署情况，本季度新增了新疆政务服务网，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 **16282** 张，比上一季度减少了 5.10%，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 1435 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准备好具体应对对策，这是非常有价值的数据。

16282 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	12,655	3,443	184
占比	77.72%	21.1%	1.13%

表 2

签发这 16282 张 SSL 证书的 SSL 证书提供商前 20 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。可以看出我国拥有自己的顶级根 CA 的签发比例仅占 6.29%，而且上海 CA 的根还需要波兰 CA 的交叉签名，国外 CA 占比高达 93.71%。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 5.29%的增长。

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	8,811	54.11%	-7.23%	DigiCert (美国)	
2	亚数信息	中国	2,594	15.93%	-13.99%	Sectigo/DigiCert (美国)	
3	Let's Encrypt	美国	796	4.89%	5.29%	ISRG (美国)	自动化部署
4	数安时代	中国	646	3.97%	0.31%	Assecods + GDCA (波兰 + 中国)	
5	沃通CA	中国	633	3.89%	-4.67%	Sectigo/DigiCert/Assecods (美国/波兰)	
6	中金认证	中国	606	3.72%	-0.16%	CFCA (中国)	
7	上海CA	中国	419	2.57%	6.35%	Assecods x UniTrust (中国)	
8	北京信查查	中国	410	2.52%	27.33%	Assecods/Sectigo (波兰/美国)	
9	GlobalSign	日本	382	2.35%	5.82%	GlobalSign (日本)	
10	Sectigo	美国	319	1.96%	2.90%	Sectigo (美国)	
11	天威诚信	中国	147	0.90%	3.52%	Assecods (波兰)	
12	上海锐成	中国	116	0.71%	20.83%	Sectigo (美国)	
13	合肥网盾	中国	74	0.45%	39.62%	Sectigo (美国)	
14	Cloudflare	美国	59	0.36%	3.51%	DigiCert (美国)	
15	腾讯云	中国	56	0.34%	14.29%	Sectigo (美国)	
16	ZeroSSL	奥地利	46	0.28%	-6.12%	Sectigo (美国)	
17	北京新网	中国	45	0.28%	60.71%	Sectigo (美国)	
19	深圳CA	中国	37	0.23%	0.00%	Assecods (波兰)	
19	Assecods	波兰	17	0.10%	-10.53%	Assecods (波兰)	
20	其他		69	0.42%	25.45%	国外CA	
合计			**16,282**				

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 **16282** 张，连续两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。

	证书数量	检索域名	默认https	启用国密	WAF防护	安全评级
中国大陆	**16282**	*.gov.cn	是	否	有	B+
中国台湾省	**12483**	*.gov.tw	是	否		B+
中国香港特别行政区	**1997**	*.gov.hk	是	否		B+
中国澳门特别行政区	**440**	*.gov.mo	是	否		B+

表 4

三、我国十大银行网站的 SSL 证书统计数据分析

从本期开始增加我国二十大银行域名的 SSL 证书申请量统计数据，见下表 5，这 20 家银行名单来自中国银行业协会 2023 年 8 月发布的年度“中国银行业 100 强榜单”，有些银行不止一个域名，为了统计方便只采用了其中一个主要域名的统计数据。由于 SSL 证书提供商有很多家，鉴于表格宽度有限，我们仅列出了市场份额排名的前两名，正好一家是美国 CA，一家

是中国 CA，其他家的数据统一合并在“其他 CA”中，这些“其他 CA”基本上都是国外 CA，所以，同美国 CA 一起统计在“国外 CA%”中。

排名	银行名称	检索域名	证书数	DigiCert(美)	中金认证(中)	其他CA	国外CA%	国密证书	全站HTTPS
1	工商银行	icbc.com.cn	672	652	16	4	97.62%	有	是
2	建设银行	ccb.com	562	266	222	74	60.50%	无	不是
3	农业银行	abchina.com	81	78		3	100.00%	有	是
4	中国银行	boc.cn	224	221		3	100.00%	有	是
5	交通银行	bankcomm.com	75	11	1	63	98.67%	无	不是
6	招商银行	cmbchina.com	338	330		8	100.00%	无	是
7	邮储银行	psbc.com	124	25	81	18	34.68%	有	不是
8	兴业银行	cib.com.cn	271	271			100.00%	是	是
9	浦发银行	spdb.com.cn	82	45	36	1	56.10%	无	是
10	中信银行	ecitic.com	139	138		1	100.00%	无	不是
11	民生银行	cmbc.com.cn	28			28	100.00%	无	不是
12	光大银行	cebbank.com	78	39	27	12	65.38%	无	不是
13	平安银行	pingan.com.cn	161	145		16	100.00%	无	不是
14	华夏银行	hxb.com.cn	121	23	69	29	42.98%	无	是
15	北京银行	bankofbeijing.com.cn	108	62	19	27	82.41%	有	是
16	广发银行	cgbchina.com.cn	17	15		2	100.00%	无	不是
17	上海银行	bankofshanghai.com	5	3	1	1	80.00%	无	是
18	江苏银行	jsbchina.cn	9	4		5	100.00%	无	不是
19	宁波银行	nbcb.com.cn	14	8		6	100.00%	无	不是
20	浙商银行	czbank.com	49	49			100.00%	有	不是
合计			**3,158**	**2,385**	**472**	**301**	**85.05%**	**7**	**9**

表 5

从上面的统计数据可以看出我国银行网银系统 HTTPS 加密安全存在如下三个方面的主要问题，希望这些统计数据能引起金融监管部门和各个银行的高度重视。

1. 我国网银系统中采用美国 CA-DigiCert 的比例高达 75.52%，也就是原先的 VeriSign 被赛门铁克收购后又被 DigiCert 收购的 CA，加上其他国外 CA，比例高达 85.05%，这意味者我国网银系统也一样面临俄罗斯银行一样的安全风险。

2. 我国银行业是最早要求国密改造的行业，但是在前 20 大银行的网银系统中，只有一家银行默认启用国密 HTTPS 加密，还有 6 家部分网银系统支持国密 HTTPS 加密，而这 6 家中有两家用的自签证书，一家的证书有效期为 3 年，这 3 家即使使用了国密证书，但由于不受信任而使得零信浏览器为了用户体验而自动采用 RSA 算法实现 HTTPS 加密，因为 RSA 算法 SSL 证书是可信证书。只有 1 家银行官网部署了零信浏览器信任的国密 SSL 证书而默认采用国密算法实现 HTTPS 加密，这是完全符合有关银行安全规范要求的，有 6 家银行的部分系统满足合规要求，其他银行都是不符合合规要求的。

3. 20 家银行官网中只有 9 家是默认 HTTPS 加密的，有些银行官网甚至没有启用 HTTPS 加密，这也是严重不合规的、也是用户不可接受的严重安全问题，特别是有些银行的银

行卡查询业务系统居然没有启用 HTTPS 加密，则非常不安全，因为大量用户的查询口令同取款口令是一样的，没有实现 HTTPS 加密而导致的用户钱财损失可不是用户保管口令不善导致的，而且银行提供的查询功能不安全导致的。

四、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，仅排名为第五和第六，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 17 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 17 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 6 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(下表中表示为“+”)。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 **129.4598** 万张，比上一季度减少了 **11.46%**，对比全球数据减少了 5.77%，说明国内 SSL 证书提供商的市场份额连续两个季度在下降，这 17 家的总和在全球 SSL 证书提供商中排名第 **14** 位，比上个季度上升了一位。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，早介入早收益。

排名	公司名称	有效证书数	增长%	顶级根
1	亚数信息	1,237,387	-12.32%	Sectigo/DigiCert
2	北京信查查	12,887	3.65%	Assecods/Sectigo
3	上海锐成	10,062	52.41%	Sectigo
4	沃通CA	9,428	-2.32%	Sectigo/Assecods/DigiCert
5	腾讯云	4,500	17.99%	Sectigo
6	合肥网盾	3,965	7.66%	Sectigo
7	中金认证	3,799	-1.32%	CFCA
8	上海CA	3,595	8.77%	Assecods x UniTrust
9	天威诚信	2,280	-3.96%	Assecods
10	证签零信	1,542	26.50%	Sectigo
11	北京新网	1,351	53.70%	Sectigo
12	数安时代	1,295	0.62%	Assecods + GDCA
13	百度云	951	5.43%	Sectigo
14	浙江葫芦娃	775	32.48%	Sectigo
15	阿里云	454		GlobalSign
16	北京中万	183	35.56%	Sectigo
17	深圳CA	144	-2.70%	Assecods
合计		**1,294,598**	**-11.46%**	

表 6

五、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 **2118** 张，比上一季度略有小幅增长。

这里提醒零信浏览器信任的 CA 机构注意：零信浏览器计划推出的强制实施国密证书透明计划的日期从原计划的 2023 年 7 月 1 日推迟到 2024 年 1 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 1 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，我们希望有更多家机构，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。

六、统计数据亮点和问题分析

本期统计数据有 3 个亮点，一是增加了银行网银系统 SSL 证书的申请量统计数据，统计

表明，我国网银系统不仅存在较高的安全风险，而且存在大量不合规的情况，这个值得相关部门和单位高度重视。本次统计只统计了前 20 家银行，而我国有三千多家银行，前 20 家银行的情况都不乐观，其他小银行就更不乐观了。

第二亮点是 17 家 SSL 证书提供商上，有 5 家公司出现了负增长，而巧的是这 5 家负增长机构全部都是拥有工信部和国密局 CA 许可证的公司，这就值得各个 CA 机构深思和反省了。国际 SSL 证书业务目前在我国是一个完全开放的市场，所有非 CA 机构的积极渗透和灵活的市场策略都值得各 CA 机构学习和反思。各 CA 机构应该抓住国密 SSL 证书的未来市场，毕竟这个市场的用户还是看好 CA 机构的合规资质的，抓住这个给用户提供国密 SSL 证书的同时配套提供国际 SSL 证书的机会，实现双 SSL 证书的部署，只要这样才可能借国密 SSL 证书市场的成功而同时赢得国际 SSL 证书的市场。

第三个亮点是还是自动化证书管理，这仍然是 SSL 证书提供商必须抓住的机会。在全球市场，传统 CA 机构 Sectigo 在前 4 位签发数量都有一定的减少的情况下有 5.65%的增长，而另一家 CA 机构 GoDaddy 则更猛，增加了 216%，从 9 位上升到第 7 位，这是因为这两家 CA 机构也开始支持 ACME，Sectigo 提供 SCM 服务能帮助用户扫描整个证书透明日志数据库来发现本单位所申请的所有 SSL 证书，集中管理并及时自动化续期和续费，实现了全自动化证书管理，这值得我国 CA 机构学习。国际 CA 机构市场份额的增长与国内 CA 机构的市场份额的减少形成了巨大的反差，还是那句话，CA 机构或者 SSL 证书提供商一定要大胆拥抱自动化证书管理，大胆采用 HTTPS 加密自动化的解决方案，只有这样才能赢得未来市场。

七、小结

本期报告在中秋国庆双节假期完成，那就用零信任研究院发布的双节海报主题来做小结-“**商密保国安，岁岁享团圆**”，只有普及应用商用密码才能保障我国网络空间安全，只有普及国密 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。

为了国家的长治久安，密码人继续齐加油！祝大家有一个美美的双节假期。

零信技术（深圳）有限公司
数字签名者：零信技术（深圳）有限公司
日期：2023.10.03 10:56:16 +08'00'

请关注公司公众号，实时推送公司 CEO 精彩博文。