中国 SSL 证书市场发展趋势分析简报-2023Q2

零信任安全研究院全球独家发布

(2023 年 7 月 5 日)

本报告由零信技术零信任安全研究院发布，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、有数字签名和时间戳的 PDF 版本)。

本次发布的是定期发布的 2023 年第二季度分析报告，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。本次简报特别发布了全球 CA 为我国政府域名*.gov.cn 签发的 SSL 证书的数据，很惊人！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 7 月 1 日**，已经在国际证书透明日志系统记录的全球 SSL 证书总数突破 **98 亿**张(98.3886 亿)，其中未过期的有效 SSL 证书有 **6.5195** 亿张，比上一季度增长了 **25.60%**，增长幅度不少，说明全球经济在疫情过后正在快速复苏中。

全球 **6.5195 亿**张有效证书中，只验证域名的 DV SSL 证书有 **5.4329 亿**张，占比 **83.33%**，比第一季度增长了 **30.08%**。验证网站身份的 OV SSL 证书有 **1.0818 亿**张，比上一季度增长 **7.07%**，占比 **16.59%**，占比比第一季度下降了 **2.88%**。扩展验证网站身份的 EV SSL 证书 **35.996 万张**，比上一季度增长 **4.01%**，占比 **0.08%**，这是连续 4 个季度第一次增长，不知道是否与零信浏览器在全球市场占有率的持续增长有关，因为目前全球只有零信浏览器显示 EV SSL 证书为绿色地址栏而突显 EV SSL 证书的价值。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 **6.5195 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 (3.2990 亿张)、第 2 位是 Cloudflare (6305 万张)、第 3 位是谷歌 (5606 万张)、第 4 位是亚马逊 (5066 万张)、第 5 位是 Sectigo 4009 万张)、第 6 位是 DigiCert (3230 万张)、第 7 位是微软 (2262 万张)、第 8 位是 cPanel (1719 万张)、第 9 位是 GoDaddy (1191 万张)、第 10 位是 ZeroSSL (1048 万张)。对比上一季度的数据，谷歌从第 4 位上升到第 3 位，亚马逊从第 3 名下降到第 4 位。

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。

而这 8 家互联网和云服务提供商签发的所有 SSL 证书都是自动化签发和部署的，占比高达 **86%**，这个比例更是值得我国互联网服务提供商、云服务提供商、CA 机构(SSL 证书提供商)的深思，如果大家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。

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 **1736** 张，比上一季度增长 **25.98%**，这是本季度最大的亮点，31 个省市自治区中有 26 个省区都在增长，3 个维持不变，只有两个略有下降，其中浙江省、江西省、山东省、福建省、山西省、辽宁省和西藏自治区共 7 个省区的增幅超过 **50%**，这说明各省政务网站开始真正行动起来了，开始大量部署 SSL 证书来保障政务系统安全，这个必须点赞。排名前 5 位的是**浙江省、上海市、北京市、广西壮族自治区、江西省。**

在国际算法 SSL 证书申请量大幅增长 26%的同时国密算法 SSL 证书不但没有增长，反而有下降，31 个省市自治区省级政府官网中部署了国密 SSL 证书的只有一个湖南省政府门户网站。

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	283	66.47%	*.zj.gov.cn	是	否		B+
2	上海市	167	5.03%	*.shanghai.gov.cn, *.sh.gov.cn	是	否		B
3	北京市	145	19.83%	*.beijing.gov.cn	是	否	有	
4	广西壮族自治区	101	0.00%	*.gxzf.gov.cn	否	否		
5	江西省	84	90.91%	*.jiangxi.gov.cn	否	否		
6	广东省	81	-12.90%	*.gd.gov.cn	否	否		
7	宁夏回族自治区	80	29.03%	*.nx.gov.cn	是	否		B+
8	海南省	75	22.95%	*.hainan.gov.cn	是	否		B+
9	天津市	61	1.67%	*.tj.gov.cn	是	否	有	A
10	吉林省	52	10.64%	*.jl.gov.cn	否	否	有	
11	云南省	52	44.44%	*.yn.gov.cn	是	否		B+
12	重庆市	50	28.21%	*.cq.gov.cn	否	否		
13	河南省	50	42.86%	*.henan.gov.cn	是	否		B+
14	陕西省	48	45.45%	*.shaanxi.gov.cn	否	否		
15	山东省	48	84.62%	*.shandong.gov.cn, *.sd.gov.cn	否	否		
16	甘肃省	46	9.52%	*.gansu.gov.cn	是	否		B+
17	贵州省	40	8.11%	*.guizhou.gov.cn	否	否		
18	湖南省	34	13.33%	*.hunan.gov.cn	否	有		
19	安徽省	32	-3.03%	.ah.gov.cn	是	否	有	A
20	福建省	32	68.42%	*.fujian.gov.cn, *.fj.gov.cn	是	否		B+
21	河北省	28	27.27%	*.hebei.gov.cn	否	否		
22	江苏省	20	33.33%	*jiangsu.gov.cn, *.js.gov.cn	否	否		
23	青海省	19	26.67%	*.qinghai.gov.cn	否	否		
24	新疆维吾尔自治区	19	46.15%	*.xinjiang.gov.cn	否	否		
25	黑龙江省	18	0.00%	*.hlj.gov.cn	是	否	有	A
26	山西省	18	80.00%	*.shanxi.gov.cn	是	否		B+
27	内蒙古自治区	15	36.36%	.nmg.gov.cn	是	否	有	A
28	辽宁省	14	55.56%	*.ln.gov.cn	否	否		
29	西藏自治区	13	62.50%	*.xizang.gov.cn	否	否		
30	湖北省	8	0.00%	*.hubei.gov.cn	否	否		
31	四川省	3	200.00%	*.sc.gov.cn	是	否		B+
	合计	1736	25.98%		15	1	6	

表 1

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 4 个网站同时启用了默认 https 加密，也就是只有这 4 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 **17157** 张，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 1736 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，我们就能分析可能存在的风险和具体应对对策，这是非常有价值的数据。

17157 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。

证书类型	DV SSL 证书	OV SSL 证书	EV SSL 证书
证书数量	13,508	3,474	175
占比	**78.73%**	20.25%	1.02%

表 2

签发这 17157 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 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 5.83%，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 94.17%。

排名	公司名称	国别	证书数	占比	根CA (国别)	备注
1	DigiCert	美国	9,498	55.36%	DigiCert (美国)	
2	亚数信息	中国	3,016	17.58%	Sectigo/DigiCert (美国)	
3	Let's Encrypt	美国	756	4.41%	ISRG (美国)	自动化部署
4	沃通CA	中国	664	3.87%	Sectigo/DigiCert/Assecods (美国/波兰)	
5	数安时代	中国	644	3.75%	Assecods + GDCA (波兰 + 中国)	
6	中金认证	中国	607	3.54%	CFCA (中国)	
7	上海CA	中国	394	2.30%	Assecods x UniTrust (中国)	
8	GlobalSign	日本	361	2.10%	GlobalSign (日本)	
9	北京信查查	中国	322	1.88%	Assecods/Sectigo (波兰/美国)	
10	Sectigo	美国	310	1.81%	Sectigo (美国)	
11	天威诚信	中国	142	0.83%	Assecods (波兰)	
12	上海锐成	中国	96	0.56%	Sectigo (美国)	
13	Cloudflare	美国	57	0.33%	DigiCert (美国)	
14	合肥网盾	中国	53	0.31%	Sectigo (美国)	
15	腾讯云	中国	49	0.29%	Sectigo (美国)	
16	ZeroSSL	奥地利	49	0.29%	Sectigo (美国)	
17	深圳CA	中国	37	0.22%	Assecods (波兰)	
18	北京新网	中国	28	0.16%	Sectigo (美国)	
19	Assecods	波兰	19	0.11%	Assecods (波兰)	
20	其他		55	0.32%	国外CA	
合计			**17,157**			

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 **17157** 张，首次超过了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	检索域名	默认https	启用国密	WAF防护	安全评级
中国大陆	**17157**	*.gov.cn	**是**	否	有	A
中国台湾省	**12323**	*.gov.tw	**是**	否		B+
中国香港特别行政区	**2173**	*.gov.hk	**是**	否		B+
中国澳门特别行政区	**456**	*.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 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 2 家是知名的云服务提供商，有 1 家是电信运营商，其他 8 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。

排名	公司名称	有效证书数	增长%	顶级根
1	亚数信息	1,411,221	-39.47%	Sectigo/DigiCert
2	北京信查查	12,433	-35.36%	Assecods/Sectigo
3	沃通CA	9,652	-37.56%	Sectigo/Assecods/DigiCert
4	上海锐成	6,602	45.04%	Sectigo
5	中金认证	3,850	-32.76%	CFCA
6	腾讯云	3,814	23.63%	Sectigo
7	合肥网盾	3,683	-4.86%	Sectigo
8	上海CA	3,305	-18.11%	Assecods x UniTrust
9	天威诚信	2,374	-34.15%	Assecods
10	数安时代	1,287	-31.54%	Assecods + GDCA
11	证签零信	1,219	-12.18%	Sectigo
12	百度云	902	-38.72%	Sectigo
13	北京新网	879	13.57%	Sectigo
14	浙江葫芦娃	585	-2.82%	Sectigo
15	深圳CA	148	-33.93%	Assecods
16	北京中万	135	8.00%	Sectigo
17	成都数证	77	-61.31%	Sectigo
18	联通CA	71	-10.13%	GlobalSign
合计		**1,462,237**	**-39.01%**	

表 5

这 18 家国际 SSL 证书提供商签发的有效证书数合计为 **146.2237** 万张，比上一季度减少了 **39%**，对比全球数据增长了 25.60%，说明国内 SSL 证书提供商的市场份额已经在下降，并且大多数提供商都有大幅下降，这 18 家的总和在全球 SSL 证书提供商中排名第 **15** 位，这是一个不好的市场信号，主要原因是国际上的 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。

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 **1920** 张。

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。

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 证书才能真正用于保障我国网站安全。

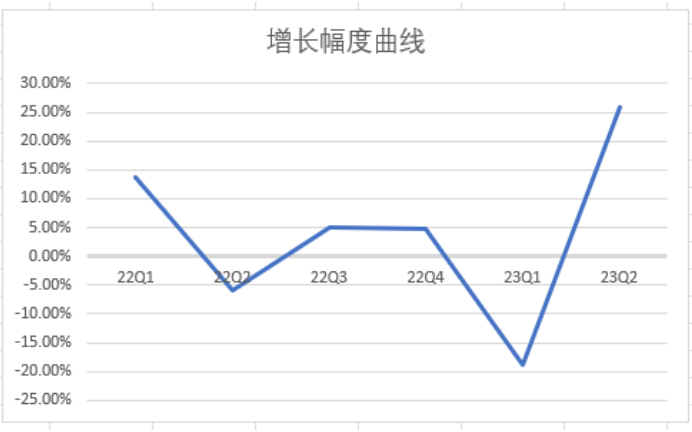
五、 统计数据亮点和问题分析

本期统计数据有 4 个亮点，一是各省政府网站的国际 SSL 证书申请量普遍有大幅度增长；二是各省政府网站的国密 SSL 证书部署量在减少；三是政府网站已经开始支持 ACME 自动化证书部署；四是本期增加了全球 CA 给我国政府网站签发的 SSL 证书的详细数据，这些数据意味着什么，下面详细分析。

1. 各省政府网站的国际 SSL 证书申请量普遍有大幅度增长

从 2022 年 Q1 到 2023 年 Q2 六个季度的增长幅度曲线可以看出，本季度我国政府网站的 SSL 证书申请量已经有了大幅度增长，并且是各省全线增长，只有两个省有小幅度的减少，虽然证书申请量还很少，但是发展趋势喜人，这充分说明了各省已经开始重视政府网站的 https 加密安全防护，以保障一网通办系统的个人和企业数据的安全，这与我国相继出台了《网络安全法》、《密码法》、《数据安全法》、《个人信息保护法》和《关键信息基础设施安全保护条例》是有密切关系的，特别是 7 月 1 日已经生效的《商用密码管理条例》，一定会进一步推动政务

网站系统的 SSL 证书的持续大量部署。



2. 各省政府网站的国密 SSL 证书部署量在减少

在国际算法 SSL 证书申请量大幅增长 26%的同时国密算法 SSL 证书不但没有增长，反而有下降，31 个省市自治区省级政府官网中部署了国密 SSL 证书的只有湖南省政府网站。为何国际 SSL 证书有大幅增长，而国密 SSL 证书的部署反而会下降，这里的关键是国密 SSL 证书缺乏普及应用的生态，不仅仅是服务器国密改造很难，而且是用户端浏览器也要更换支持国密算法。而部署一张国际 SSL 证书就比较容易了，无需任何改造，只需安装一次 SSL 证书即可。所以，国密 SSL 证书的生态建设非常重要，需要有完全免费的国密浏览器，需要有原 Web 服务器零改造实现国密 https 加密解决方案，而不仅仅是 CA 机构能签发国密 SSL 证书。

据了解，原先已经部署了国密 SSL 证书的几个省级政府网站由于系统升级，不方便改用支持国密算法的 Nginx Web 服务器，只好暂时不再部署国密 SSL 证书，这个问题凸显了零改造实现国密 https 加密的重要性和紧迫性，用户需要的是不影响现有 Web 服务器的可靠运行的国密 https 加密。推荐这些网站部署国密 HTTPS 加密自动化网关或启用国密 HTTPS 加密自动化云服务来实现零改造的国密 https 加密，尽快实现国密 https 加密，满足密评和等保合规要求，真正实现用商用密码算法来保障我国政务网站安全。

为了满足国密合规和全球信任的自适应加密算法的 https 加密应用需求，政府网站都应该部署双算法 SSL 证书(国密 SSL 证书和国际 SSL 证书)，也就是说必须是国际算法 SSL 证书和国密 SSL 证书的证书申请量同时同步增长才是正常的状态，单种算法 SSL 证书的增长仍然不是安全稳健的解决方案。

3. 全球 CA 给我国政府网站签发的 SSL 证书的详细数据分析

这是本期报告的重点，我国网站管理部门和密码管理部门并没有合适的技术手段来掌握全球 CA 何时给我国哪些网站域名签发了何种 SSL 证书，我们没有建设国家级证书透明日志系统，而基于国际证书透明日志数据查询还是有一定的技术难度的，同时国际证书透明日志系统不支持国密 SSL 证书，这就是让 SSL 证书的监管完全处于空白状态。所以，从本期开始，我们尽最大的能力从国际证书透明日志系统抽取一些为我国网站签名的 SSL 证书数据，但鉴于时间和精力有限，我们只能分析*.gov.cn 域名的签发数据，供有关部门决策参考。

从上面的统计报表 3 数据可以看出：我国.gov.cn 网站申请的 17157 张国际算法 SSL 证书中 94.17%都是由西方 CA 签发(美国、欧洲和日本)，这里是有很大的潜在安全风险的，因为已经有了前车之鉴--俄乌冲突发生后美国 CA 就吊销了俄罗斯政府和银行网站部署使用的 SSL 证书三千多张，并停止为这些网站签发新的 SSL 证书，而我国政府网站和银行网站所部署的 SSL 证书就是由西方 CA 签发的，这在目前的非常不确定的国际形势下也非常有可能遭遇被恶意吊销和断供。即使是我国 CA 完全自主签发的 3.54% 的 SSL 证书，由于自主签发证书的根证书是否能用(被信任)还是美国四大浏览器(谷歌、苹果、微软和火狐)说了算。也就是说，这个自主签发证书也是要打一个大问号的，根基不牢，还是人家说了算，因为我们签发的 SSL 证书使用的是人家说了算的 RSA 密码算法，因为整个应用生态都是基于 RSA 算法的。

唯一一个“去风险”的解决方案就是我国政府网站和银行网站全部部署国密 SSL 证书，只有国密算法 SSL 证书才是我国真正自主可控的 SSL 证书，才能真正保障我国政务网站和网银系统的安全。这是政府网站和银行网站部署 SSL 证书的下一个重点工作，也是国密合规和等保合规的要求，更是密评的要求。

4. 政府网站开始支持 ACME 自动化证书部署

在 17157 张.gov.cn 域名证书中，有一个很有意思的数据就是有 4.41%的政府网站启用了自动化部署的 Let’s Encrypt 签发的 90 天免费 SSL 证书，我们分析发现这些网站基本上都是地县级政府单位的小网站，这是一个值得注意的数据，我们认为至少有两个亮点：一是越是小单位，没有专业运维人员越能接受自动化部署 SSL 证书的方案，与部署的 SSL 证书是否是收费还是免费无关，只要能实现免维护就行。二是由于部署 Let’s Encrypt 证书需要在服务器上安装一个 ACME 客户端软件，所以只有小网站和新建的网站才愿意这么做，而正在运行的大网站则由于怕影响正在运行的业务系统而不敢这么做。所以，对于市级或省级政府的大网站就没有看到这种情况，这类网站的最佳的解决方案是部署 HTTPS 加密自动化网关的方式来解决，无需动原

服务器就可以自动化实现 https 加密。

当然，为了满足用户同时部署国密 SSL 证书和国际 SSL 证书的需求，我国政府网站应该支持国密 ACME 实现双算法双 SSL 证书的自动化部署，目前的国际 ACME 只能自动化部署国际 SSL 证书。

六、小结

本期报告晚了几天发布，主要是多花了几天时间在国际证书透明日志系统中收集整理全球 CA 给我国政府网站*.gov.cn 域名签发的 SSL 证书数据，*.gov.cn 网站属于我国关键信息基础设施网站，而 SSL 证书是为了保障政务数据安全的主要技术手段，相关主管部门在写本季度报告之前提出想了解这些数据的需求，这是本期报告新增的内容和重点内容，可供有关决策参考。

本期可喜的是政府网站 SSL 证书部署量有大幅度增长，这必将大大提升我国政务网站的安全防护水平。而很遗憾的是政府网站部署国密 SSL 证书的数量反而在减少，这与国密 SSL 证书的应用生态有非常大的关系，我们不仅需要有 CA 机构能签发国密 SSL 证书，还需要整个相关应用生态都支持国密 SSL 证书，包括但不限于有完全免费的支持国密算法的国产浏览器，有零改造实现国密 https 加密的解决方案，还要有支持国密 SSL 证书的 CDN/WAF 服务等等，打造国密 SSL 证书应用生态任重道远，需要业界齐努力，让商用密码真正能快速落地应用来保障我国互联网安全。

请关注公司公众号，实时推送公司 CEO 精彩博文。