中国 SSL 证书市场发展趋势分析简报-2023Q1

零信任安全研究院全球独家发布

(2023 年 4 月 4 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。本次简报特别发布了自动化签发的 SSL 证书的数据以及对证书有效期将缩短为 90 天的应对之策，希望这些数据和建议能为相关政府机构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

根据证书透明日志系统数据统计，截止到 **2023 年 4 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 **90 亿**张(90.4881 亿)，其中未过期的有效 SSL 证书有 **5.1907 亿**张，细心的读者一定能发现上一季度(2022 年 Q4)的数据是 **8.0213 亿**张，怎么会突然减少了 2.8306 亿张呢？这是因为从 2023 年开始我们更新了查询算法，使得这两个季度的数据没有了可比性，请读者理解为目前这个新的算法能更加准确地反映真实数据，因为谷歌已经不再要求 CA 必须提交预签 SSL 证书到谷歌自己运营的证书透明日志服务系统中，只需提交到 6 个通过谷歌认证的 3 个或 2 个之一即可，这使得分析数据和剔除重复数据算法变得很复杂，从而导致了本次报告的数据同上一季度的数据差异比较大。

全球 **5.1907 亿**张有效证书中，只验证域名的 DV SSL 证书 **4.1766 亿**张，占比 **80.46%**。验证网站身份的 OV SSL 证书有 **1.0104 亿**张，占比 **19.47%**。扩展验证网站身份的 EV SSL 证书 **34.609 万**张，占比 **0.07%**。虽然具体数据同上一期没有可比性，但是三种 SSL 证书类型的占比仍然有可比性，DV SSL 证书占比下降了了 4%，OV SSL 证书占比上升了 21%，但是我们研究发现，这个 OV SSL 证书的占比上升是由于 Cloudflare 自动化签发了大量的 O 字段等于 Cloudflare 的 OV SSL 证书，但实际上是为使用了 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，三种 SSL 证书类型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，从本期开始不再依据 OV SSL 证书和 EV SSL 证书的数据来排名全球前 30 个国家的 SSL 证书申请情况。本期将重点分析自动化申请和部署的 SSL 证书的签发数据，这个对我国如何普及 SSL 证书应用更有现实意义。

全球 **5.1907 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 (2.5269 亿张)、第 2 位是 Cloudflare (6156 万张)、第 3 位是亚马逊 (4446 万张)、第 4 位是谷歌 (3727 万张)、第 5 位是 Sectigo (3157 万张)、第 6 位是 DigiCert (3076 万张)、第 7 位是微软 (2086 万张)、第 8 位是 cPanel (1398 万张)、第 9 位是 GoDaddy (800 万张)、第 10 位是 ZeroSSL (783 万张)。对比上一季度的数据，亚马逊从第 6 位上升到第 3 位，上升幅度不少，这与其云服务市场份额提升和免费自动化配置 SSL 证书是有密切关系的。

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。

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 **88%**，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 88%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。

SSL 证书的有效期从 5 年，逐渐缩短到 3 年、2 年、1 年，现在的情况是一年期 SSL 证书基本上是收费的，而 90 天有效期的 SSL 证书都是免费的，如果只能签发 90 天有效期的 SSL 证书标准开始实施，则还会有用户会花钱去购买收费的 90 天有效期证书吗？这值得所有 SSL 证书提供商思考如何应对这个变化，也非常值得 SSL 证书用户思考如何应对每 90 天必须申请

和部署 SSL 证书。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域名就能得到这个省的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。

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 **1378** 张，排名前 5 位的是**浙江省、上海市、北京市、广西壮族自治区、广东省。**本次统计发现有多个省政府门户网站虽然部署了 SSL 证书，但是并没有设置为自动启用 https 加密，这等于没有部署 SSL 证书，因为用户并不会手动在地址栏输入 https 加网址的，这个值得高度重视。美国联邦零信任战略要求所有.gov 域名的政府网站只能用 https 加密方式访问，这是网站安全的基础，没有这个基础其他任何安全防护措施和防护系统则形同虚设，因为 https 加密保护的是用户的数据不会在网络传输过程中被泄露和被篡改，这是安全木桶的底板，底板都没有其他侧板没有存在的价值！

31 个省市自治区省级政府官网中部署了国密 SSL 证书的有江西省政府官网和湖南省政府网站，但是由于这两个网站并没有设置默认启用 https 加密，所有国密算法并没有真正用于保护政府网站安全，这个国密 SSL 证书的部署也等于没有部署！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。

排名	省市自治区	证书数量	检索域名	默认https	部署国密	WAF防护	安全评级
1	浙江省	170	*.zj.gov.cn	是	否		B+
2	上海市	159	*.shanghai.gov.cn, *.sh.gov.cn	是	否		B
3	北京市	121	*.beijing.gov.cn	否	否	有	
4	广西壮族自治区	101	*.gxzf.gov.cn	否	否		
5	广东省	93	*.gd.gov.cn	否	否		
6	宁夏回族自治区	62	*.nx.gov.cn	是	否		B+
7	海南省	61	*.hainan.gov.cn	是	否		B+
8	天津市	60	*.tj.gov.cn	是	否	有	A
9	吉林省	47	*.jl.gov.cn	否	否	有	
10	江西省	44	*.jiangxi.gov.cn	否	有		
11	甘肃省	42	*.gansu.gov.cn	是	否		B+
12	重庆市	39	*.cq.gov.cn	否	否		
13	贵州省	37	*.guizhou.gov.cn	否	否		
14	云南省	36	*.yn.gov.cn	是	否		B+
15	河南省	35	*.henan.gov.cn	是	否		B+
16	陕西省	33	*.shaanxi.gov.cn	否	否		
17	安徽省	33	.ah.gov.cn	是	否	有	A
18	湖南省	30	*.hunan.gov.cn	否	有		
19	山东省	26	*.shandong.gov.cn, *.sd.gov.cn	否	否		
20	河北省	22	*.hebei.gov.cn	否	否		
21	福建省	19	*.fujian.gov.cn, *.fj.gov.cn	是	否		B+
22	黑龙江省	18	*.hlj.gov.cn	是	否	有	A
23	江苏省	15	*jiangsu.gov.cn, *.js.gov.cn	否	否		
24	青海省	15	*.qinghai.gov.cn	否	否		
25	新疆维吾尔自治区	13	*.xinjiang.gov.cn	否	否		
26	内蒙古自治区	11	.nmg.gov.cn	是	否	有	A
27	山西省	10	*.shanxi.gov.cn	是	否		B+
28	辽宁省	9	*.ln.gov.cn	否	否		
29	西藏自治区	8	*.xizang.gov.cn	否	否		
30	湖北省	8	*.hubei.gov.cn	否	否		
31	四川省	1	*.sc.gov.cn	是	否		B+
	合计	1378		14	2	6	

我们检索了 ***.gov.cn** 的 SSL 证书申请量为 **3537** 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 1378 张。而根据中国互联网络信息中心 2022 年 8 月 31 日发布的第 50 次《中国互联网络发展状况统计报告》的数据，截至 2021 年 12 月，我国共有政府网站 **14566** 个，也就是说，我国政府网站的 SSL 证书申请比例只有将近 **24%**，比上一季度的数据有所下降。

我们同时还检索了港澳台地区的 SSL 证书申请量，如下表所示。我国大陆各省市所有政府网站合计证书申请量为 **3537** 张，对比港澳台的数据还是很少的，这从另一个方面说明了我国大陆地区的政府网站还需要进一步增强安全防护意识，在已经普及一网通办的基础上扎实做好网站安全防护和数据加密保护工作，只有这样才能为老百姓提供更好更安全的电子政务服务，希望有关部门能高度重视网站安全的同步建设工作。

	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	3537	*.gov.cn	否	否		
中国台湾省	3732	*.gov.tw	是	否		B+
中国香港特别行政区	2088	*.gov.hk	是	否		B+
中国澳门特别行政区	512	*.gov.mo	是	否		B+

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。

本次列入统计的本土 SSL 证书提供商有 20 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 20 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，有 1 家是电信运营商，其他 9 家是商业公司。

而这 20 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 17 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 20 家国际 SSL 证书提供商签发的有效证书数合计为 **239.7810** 万张，总和在全球 SSL 证书提供商中排名第 **11** 位，至于前十大全球 SSL 证书提供商为我国网站签发了多少张 SSL 证书由于大量都是不含国家信息的 DV SSL 证书，所以无法统计，但可以肯定的是：我国本土 SSL 证书提供商所签发的 SSL 证书数量占比是非常低的，估计少于 **10%**。

排名	公司名称	有效证书数	增长%	顶级根
1	亚数信息	2,331,382	-16.77%	Sectigo/DigiCert
2	北京信查查	19,235	9.27%	Assecods/Sectigo
3	沃通CA	15,457	-15.54%	Sectigo/Assecods/DigiCert
4	中金认证	5,726	2.07%	CFCA
5	上海锐成	4,552	31.60%	Sectigo
6	上海CA	4,036	17.74%	Assecods x UniTrust
7	合肥网盾	3,871	19.99%	Sectigo
8	天威诚信	3,605	-7.85%	Assecods
9	腾讯云	3,085	24.45%	Sectigo
10	数安时代	1,880	10.33%	Assecods + GDCA
11	百度云	1,472	-12.38%	Sectigo
12	证签零信	1,388	-27.44%	Sectigo
13	北京新网	774	39.46%	Sectigo
14	浙江葫芦娃	602	35.59%	Sectigo
15	深圳CA	224	5.16%	Assecods
16	成都数证	199	-38.20%	Sectigo
17	北京中万	125	25.00%	Sectigo
18	广州金网安	105	1.94%	Assecods
19	联通CA	79	887.50%	GlobalSign
20	阿里云	13	116.67%	GlobalSign
合计		**2,397,810**	**-16.35%**	

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 **1865** 张。这里提醒零信浏览器信任的 SSL 证书提供商注意：从 2023 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，各家 CA 机构需要抓紧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。

五、 统计数据亮点和问题分析

1. 谷歌计划推动缩短 SSL 证书有效期为 90 天对我国 SSL 证书市场的影响

3 月 3 日谷歌浏览器在根认证计划中发布了推动国际标准缩短 SSL 证书有效期为 90 天的

计划，我们相信这个计划一定会在 CA/浏览器论坛上遭遇 CA 的反对，但是这只能推迟计划的实施，最晚明年一定能落地。这一计划不仅仅是对 CA 机构(SSL 证书提供商)有冲击，而且对 SSL 证书相关的产业界都有冲击，包括 SSL 证书用户、云服务提供商和 SSL 证书提供商，当然对普及和推广国密 SSL 证书也是一个巨大的冲击。

对于 SSL 证书用户，必须提前做好准备选择能自动化提供 SSL 证书的厂商和选择适合自己的自动化证书管理方案。特别是政务云用户，有大量的服务器都需要部署 SSL 证书，SSL 证书有效期缩短了四分之三，意味着申请和部署 SSL 证书的工作量将增加 4 倍！所以，必须提前做好准备选择合适的自动化部署方案，而不是传统的人工申请和人工安装方案。而对于同时需要部署国密 SSL 证书满足合规要求的用户，双 SSL 证书部署也只有自动化管理这一条路了，必须是零改造自动化实现国密 https 加密的方案。

对于有大量的云服务器需要部署 SSL 证书的云服务提供商，必须尽快实施 SSL 证书自动化部署方案，让用户选购云服务时默认自动化配置 SSL 证书，只有这样的云服务才能真正具有竞争力而不会在“90 天证书革命”中被淘汰！当然，必须提供双算法双 SSL 证书的自动化部署，因为用户有紧迫的国密合规需求。这是对于我国云服务提供商的一项新的挑战，从上面的国际 SSL 证书的全球市场数据可以看出，目前国际云服务提供商巨头们已经做好准备并且已经在实施自动化管理 SSL 证书，这非常值得我国云服务提供商学习。

对于 CA 机构(SSL 证书提供商)，已经提供 SSL 证书的机构必须尽快为用户提供自动化证书管理方案，并且必须是双 SSL 证书部署方案，传统的人工帮助用户申请和安装 SSL 证书的方案已经行不通了！而还没有提供 SSL 证书的 CA 机构，这是一个入场洗牌的好机会，可以没有历史负担的直接为用户提供用户喜欢的自动化管理方案，谁先提供好的自动化方案谁就能赢得市场，最后被淘汰的是当然是让用户手动申请 SSL 证书的厂商！CA 机构和有兴趣成为 SSL 证书提供商的公司必须能看到这个危机而带来的商机，有“危”才有机会！

2. 多台服务器共享同一张通配型 SSL 证书的安全问题

我们在收集和整理 SSL 证书的部署情况时发现，无论是各省政务云还是各个商业公共云，普遍存在申请和部署通配型 SSL 证书的情况(*.domain)，存在大量多个政府网站共用同一张通配证书的情况，因为各省市政务云域名采用了子域名管理方式，而通配证书正好满足了可以用于所有子域的部署需求，这是“最省钱”的方案—“一张证书搞定所有政务网站”。

但是，这种部署方案存在巨大的安全隐患，如果这张通配证书私钥被泄露，则 CA 必须吊销这张证书，就会导致全省各局委办的所有网站都无法使用 https 加密服务，必须重新为所有

服务器一一部署 SSL 证书，这个重新部署 SSL 证书的工作量和对政务业务的影响是巨大的，是一个不省钱的方案！但是，如果每一个政务网站部署的是独立密钥的 SSL 证书，则某一个网站的密钥泄露不会对整个省的其他政务网站有任何影响。这个不安全的能表面上好像省钱的方案实际上根本不省钱，更费钱和损失更大！而为了应对像俄罗斯那样的 SSL 证书被非法吊销的极端情况，政务网站不仅应该实现“一站一证”，而且必须从不同的 SSL 证书提供商采购 SSL 证书，以尽量减少可能的证书被非法吊销的风险，这也是古人留给我们的智慧—“鸡蛋不能放在一个篮子里”。同理，所有政务网站的安全不能依赖于一张 SSL 证书，必须是多张来自不同 SSL 证书提供商的通配证书！

而对于云服务提供商，这个安全问题也非常普遍。如某里云部署的 SSL 证书居然是有两百多个通配域名的多域证书，这张 SSL 证书用于所有云服务，这非常危险，一旦这张 SSL 证书的私钥在某台云服务器上被泄露，则整个云服务都会受到停服影响。这可不是什么省钱的好方案，是一个非常糟糕的非常不省钱的方案。不仅如此，这张绑定两百多个通配域名的 SSL 证书文件非常大，直接导致用户浏览器同服务器的握手流量增加了 4 倍，不仅浪费了机房带宽和用户手机流量，而且由于增加延时而大大降低了用户体验。这绝对是一个错误的得不偿失的证书部署方案！早在 2015 年微软云中国就采用了“一机一证”的部署方案，这非常值得我国云服务提供商学习！

3. 部署同一张通配型 OV SSL 证书导致的身份不匹配的问题

这个问题是第 2 个问题而导致的另一个问题，第 2 个问题中用户部署的可能是 DV 通配证书或 OV 通配证书。而如果是 OV 通配证书，则证书中的 O 字段只能是一个单位名称。我们发现多个省政务云部署的 OV 通配证书中的 O 字段是一个公司名称，这就导致了零信浏览器在地址栏显示证书中的 O 字段时会显示这个省政府网站的单位名称居然是一个公司！这可不是零信浏览器的问题，是证书中绑定 O 字段的问题。

即使是正确的 O 字段的 SSL 证书，由于是通配证书，这个 O 字段信息在政府门户网站是正确的，但是由于这张通配证书用于所有各个局委办就又是牛头不对马嘴了。所以说，OV 通配证书的滥用不仅有安全隐患而且还要身份错误和误导用户的问题，必须采用“一站一证”方案，每个局委办使用独立私钥和独立正确的身份的 OV SSL 证书，这样不仅能保证私钥安全，而且能保证网站身份真实可信。

六、小结

本次报告晚了几天发布，除了必须改变证书透明日志数据的统计方法外，我们还在纠结是否继续采用统计 OV SSL 证书和 EV SSL 证书的方法来对世界各国的 SSL 证书申请情况排名，因为大量的自动化部署的 OV SSL 证书的 O 字段信息是不正确的，实际上是 DV SSL 证书，这些数据的变化导致我们最终痛苦地决定不再依据这些数据来排名了。

本次报告的重点是希望读者能高度重视即将到来的 SSL 证书缩短为 90 天，我们称之为“90 天证书革命”，这个改变不仅对 SSL 证书相关产业有巨大影响，甚至对整个互联网安全产业都有巨大影响，如果不能及时采取应对措施，可能到时会出现多个重要网站由于忘了证书续期而导致无法访问的安全事件频发，这个变化也会导致普及国密 SSL 证书应用更加困难，业界必须提出应对措施。

另外，我们认为：要想快速普及国密 SSL 证书使用，必须有更多的 SSL 证书提供商参与到这个市场中来，所以我们坚决反对目前有些 CA 机构计划或提议限制非 CA 机构签发和销售国密 SSL 证书的想法，国际 SSL 证书在我国已经是面向全球 CA 和 SSL 证书提供商开放的市场，为何急需发展的国密 SSL 证书不能是一个开放的市场呢？封闭市场只会是扼杀创新和给国外 CA 拓展国密 SSL 证书市场提供机会，对我国的国密 SSL 证书的快速健康发展没有任何好处！

零信任安全研究院把 2023 年定义为“国密 HTTPS 加密元年”，我们非常看好国密算法 HTTPS 加密的普及应用，国际算法 SSL 证书市场被国外 CA 牢牢控制这已成为现实而且无法超越，因为我们没有话语权。而我们有话语权的国密 SSL 证书必须也一定能在业界的共同努力下实现创新快速发展，把失去的 SSL 证书市场夺回来，并牢牢掌握在我国中国人自己的手中，只有这样才能真正保障我国互联网安全！

请关注零信任安全研究院公众号，实时接收精彩文章。