中国 SSL 证书市场发展趋势分析简报-2022Q4

零信任安全研究院全球独家发布

(2023 年 1 月 1 日)

本报告从本期开始改由零信技术**零信任安全研究院**发布，仍然在零信官网 CEO 博客栏目和零信任安全研究院微信公众号：zotrusi 同时上线发布电子版。

本次发布的是定期发布的 2022 年第四季度分析报告，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。本次简报首次发布了国密 SSL 证书的签发数据，同时增加了国际 SSL 证书的国内供应商签发的国际 SSL 证书的统计数据。希望这些数据能为相关政府机构和商业机构的相关决策提供真实数据参考。

一、 全球 SSL 证书统计数据分析

根据谷歌证书透明日志系统数据统计，截止到 **2022 年 12 月 31 日**，全球有效 SSL 证书有 **8.0213 亿**张，同第三季度的数据相比减少了 **2%**，其中只验证域名的 DV SSL 证书 **6.7224 亿**张，占比 **83.81%** 略有下降。验证网站身份的 OV SSL 证书有 **1.2930 亿**张，占比 **16.12 %**，总量有上升和同上期相比的占比也略有上升。扩展验证网站身份的 EV SSL 证书 **54.929 万**张，占比 **0.07%**，同上期相比下降了 **3.6%**，4 个季度持续下降，这个下降同多家浏览器不再显示 EV SSL 证书为绿色地址栏有密切关系，希望零信浏览器的绿色地址栏的强势回归能对提升用户对 EV SSL 证书的购买信心起到促进作用。而 DV SSL 证书中，免费的 ACME 自动化管理的 SSL 证书总量为 **6.8384 亿**张，占比 **85.25%**，这是由于有多个云服务提供商都支持了自动化证书管理，而不仅仅是 Let's Encrypt 一家，从连续的 4 个季度的数据来看，SSL 证书的自动化管理已是大势所趋，全球 SSL 证书中自动化管理的比例已经超过 85%！

由于 DV SSL 证书中没有国家字段，所以笔者无法直接从证书透明日志数据库中获取 DV SSL 证书中有多少张证书是中国用户申请的，目前还没有精力把我国的 IP 地址和域名编程扫描获得 DV SSL 证书的部署统计数据。所以，现在仍然只能比较 SSL 证书国家字段为 CN 的统计数据，也就是只能统计 OV SSL 证书和 EV SSL 证书的数据，笔者认为这两种证书的数据也能真实反映 SSL 证书申请情况。

具体统计数据如下图所示，数字为 OV SSL 证书和 EV SSL 证书总申请张数，从本期开始不再单独分别列出 OV SSL 证书和 EV SSL 证书，以万为单位，排名第一的是**美国**，占全球的

比例是 75.97%**75.21%**，第二是**德国**，占比 **11.99%**，第三位仍然是**中国**，占比 **1.81%**。同上期统计数据相比，美国略有上升%，德国下降了 6.80%(有点大)，而中国增长超过 20%，其他国家中同上期数据对比有 9 个国家是正增长，其余国家是负增长，这与全球能源危机和粮食危机对全球经济的影响是大致相同的，说明经济情况影响了用户的 SSL 证书购买力。请注意，本期统计仍然是剔除物联网用的 OV SSL 证书，其中包括 CDN 服务提供商 Cloudflare 的 8638 万张、微软云的 1957 万张、思科的 46 万张。这个数据虽然没有被笔者纳入统计比较表中，但是从另一侧面说明了云服务和物联网设备的 SSL 证书部署在美国得到了飞速发展，这非常值得我国的云服务提供商和物联网学习和借鉴，目前我国的物联网设备基本上都还是 http 明文传输，非常不安全，非常容易遭遇攻击而使得物联网数据被非法窃取，甚至让物联网设备瘫痪，必须引起相关方的高度重视，必须尽快普及应用 SSL 证书来保障物联网安全！

		合计(万)	增长%	占比
1	美国	1741.14	1.43%	**75.97%**
2	德国	255.00	-6.80%	**11.13%**
3	**中国**	**49.50**	20.06%	**2.16%**
4	法国	31.48	-1.53%	1.37%
5	英国	28.54	-1.07%	1.25%
6	日本	26.62	0.57%	1.16%
7	加拿大	19.89	-0.30%	0.87%
8	荷兰	19.72	-3.80%	0.86%
9	瑞士	12.84	-22.88%	0.56%
10	意大利	11.28	1.99%	0.49%
11	澳洲	10.99	-2.83%	0.48%
12	西班牙	9.99	0.81%	0.44%
13	比利时	9.71	13.70%	0.42%
14	瑞典	7.28	-7.73%	0.32%
15	韩国	6.01	-2.12%	0.26%
16	印度	5.75	1.23%	0.25%
17	奥地利	5.35	5.94%	0.23%
18	芬兰	4.97	0.00%	0.22%
19	巴西	4.65	0.00%	0.20%
20	挪威	4.28	-0.47%	0.19%
21	波兰	3.71	3.06%	0.16%
22	中国香港	3.08	-4.35%	0.13%
23	捷克	3.05	-0.97%	0.13%
24	丹麦	2.89	1.76%	0.13%
25	新加坡	2.82	-2.42%	0.12%
26	俄罗斯	2.63	-2.59%	0.11%
27	南非	2.47	-1.20%	0.11%
28	葡萄牙	2.46	2.07%	0.11%
29	墨西哥	1.99	-3.40%	0.09%
30	阿联酋	1.92	-0.52%	0.08%

同上期数据相比，我国同前两名的美国和德国差距还很大，但增长速度较快！我国的网站数量基本上同美国的网站数量持平，但是 SSL 证书部署量却只是美国的 **2.84%**，差距非常大！也就是说，我国 SSL 证书市场机会巨大，可以说仍然是一个正在快速增长的蓝海市场！

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 **1696** 张，比上个季度增长了 **4.69%**。但是，有 9 个省市是同比下降的，其余增长的省市中黑龙江省增幅超过 50%，广西、河南、福建、江苏、新疆、内蒙古的排名上升了一位，江西上升了两位，黑龙江上升了3位，陕西上升了4位，说明这些省加强了密码合规建设和重视保护政务网站机密信息安全。排名前 5 位的是**浙江省、北京市、上海市、壮族自治区、广东省。**

排名	省市自治区	证书数量	增长%	检索域名	默认https	启用国密	WAF防护	安全评级
1	浙江省	262	1.16%	*.zj.gov.cn	是	否	无	B+
2	北京市	161	-1.83%	*.beijing.gov.cn	否	否		
3	上海市	161	3.87%	*.shanghai.gov.cn, *.sh.gov.cn	是	否	无	B
4	广西壮族自治区	115	43.75%	*.gxzf.gov.cn	否	否		
5	广东省	96	9.09%	*.gd.gov.cn	是	否	无	B+
6	江西省	77	8.45%	*.jiangxi.gov.cn	是	是	无	B+
7	宁夏回族自治区	76	2.70%	*.nx.gov.cn	是	否	无	B+
8	海南省	75	-3.85%	*.hainan.gov.cn	是	否	无	B+
9	天津市	71	9.23%	*.tj.gov.cn	是	否	有	A
10	吉林省	57	-5.00%	*.jl.gov.cn	是	否	有	A
11	云南省	52	-3.70%	*.yn.gov.cn	是	否		
12	甘肃省	47	2.17%	*.gansu.gov.cn	是	否		B+
13	重庆市	46	2.22%	*.cq.gov.cn	是	否	无	B+
14	山东省	46	17.95%	*.shandong.gov.cn, *.sd.gov.cn	否	否		
15	贵州省	38	0.00%	*.guizhou.gov.cn	是	否	无	B+
16	陕西省	34	30.77%	*.shaanxi.gov.cn	否	否		
17	河南省	31	10.71%	*.henan.gov.cn	是	否	无	B+
18	湖南省	30	-3.23%	*.hunan.gov.cn	否	否		
19	河北省	28	0.00%	*.hebei.gov.cn	否	否		
20	安徽省	27	0.00%	.ah.gov.cn	是	是	有	A
21	黑龙江省	26	52.94%	*.hlj.gov.cn	是	否	有	A
22	福建省	22	15.79%	*.fujian.gov.cn, *.fj.gov.cn	是	否	无	B+
23	山西省	21	-4.55%	*.shanxi.gov.cn	是	否		B+
24	江苏省	19	11.76%	*jiangsu.gov.cn, *.js.gov.cn	是	否	无	B+
25	青海省	18	-21.74%	*.qinghai.gov.cn	否	否		
26	新疆维吾尔自治区	16	6.67%	*.xinjiang.gov.cn	是	否	无	B+
27	内蒙古自治区	15	15.38%	.nmg.gov.cn	是	否	有	A
28	西藏自治区	10	11.11%	*.xizang.gov.cn	是	否	无	B+
29	湖北省	9	-40.00%	*.hubei.gov.cn	是	否	无	B+
30	辽宁省	9	-30.77%	*.ln.gov.cn	否	否		
31	四川省	1	0.00%	*.sc.gov.cn	是	否	无	B+
	合计	1696	4.69%		23	2	5	

31 个省市自治区省级政府官网启用国密 SSL 证书只有江西省政府官网和安徽省政府官网，继续特别表扬点赞。对于省政府官网是否有云 WAF 防护这一项，31 个省市自治区中只有 5 个省政府网站有安全防护，这方面也还有很大的提升空间，因为一个网站的安全光有 https 加密是不够，还需要有云 WAF 防护。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。本次统计还增加一个“安全评级”项，这个评级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。

为了对比我国政府网站同美国政府网站的差距，我们检索到所有***.gov.cn** 的 SSL 证书申请量为 **4280** 张，同上期相比下降了 **2.08%**，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 1696 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 **30%**。

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 **4280**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	增长%	检索域名	默认https	启用国密	WAF防护	安全评级
中国大陆	4280	-2.08%	*.gov.cn	是	否	有	A
中国台湾省	3802	-1.99%	*.gov.tw	是	否	无	B+
中国香港特别行政区	2103	0.81%	*.gov.hk	是	否	无	B+
中国澳门特别行政区	534	-2.38%	*.gov.mo	是	否	无	B+

三、 我国本土国际 SSL 证书提供商的统计数据分析

从本期开始，增加本土国际 SSL 证书提供商的证书签发数量统计数据，这些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，排名第一、第二、第四、第六、第八位都是全球知名的互联网巨头。

本次列入统计的本土 SSL 证书提供商有 21 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 21 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 10 家都是商业公司。

而这 21 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 18 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 21 家国际 SSL 证书提供商签发的有效证书数合计为 **286.6624** 万张，总和在全球 SSL 证书提供商中排名第 **11** 位，前 10 位分别是 Let’s Encrypt (4.4584 亿张)、Cloudflare (8641 万张)、DigiCert (4459 万张)、谷歌 (4361 万张)、Sectigo (4347 万张)、亚马逊 (3896 万张)、cPanel (3047 万张)、微软 (2170 万张)、ZeroSSL (1685 万张)、GoDaddy (1021 万张)。至于这十大全球 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	顶级根
1	亚数信息	2,801,284	Sectigo/DigiCert
2	沃通CA	18,301	Sectigo/Assecods/DigiCert
3	北京信查查	17,603	Assecods
4	中金认证	5,610	CFCA
5	天威诚信	3,912	Assecods
6	上海锐成	3,459	Sectigo
7	上海CA	3,428	Assecods x UniTrust
8	合肥网盾	3,226	Sectigo
9	腾讯云	2,479	Sectigo
10	证签零信	1,913	Sectigo
11	数安时代	1,704	Assecods + GDCA
12	百度云	1,680	Sectigo
13	北京新网	555	Sectigo
14	浙江葫芦娃	444	Sectigo
15	成都数证	322	Sectigo
16	深圳零信	274	Sectigo
17	深圳CA	213	Assecods
18	广州金网安	103	Assecods
19	北京中万	100	Sectigo
20	联通CA	8	GlobalSign
21	阿里云	6	GlobalSign
合计		2,866,624	

四、 我国国密 SSL证书提供商的统计数据分析

从本期开始，除了增加本土国际 SSL 证书提供商的证书签发数量统计数据外，还对比增加我国国密 SSL 证书提供商的统计数据分析。我们认为：国际 SSL 证书的话语权在国外，所以我国本土国际 SSL 证书提供商受到了多重因数的制约而无法获得应有的品牌和市场份额，国际 SSL 证书只是为了兼容现在的基于 RSA 密码体系的系统的兼容而存在，真正的未来市场应该是我国自主密码算法的国密 SSL 证书，我国互联网安全应该也必须由国密 SSL 证书来保障，俄乌冲突导致的大量国际 SSL 证书的吊销和断供这种特大安全事件和教训不能也不应该在我国将来的某个时刻重演！我国 SSL 证书的未来主流产品应该是国密 SSL 证书。所以，从本期开始，本报告增加国密 SSL 证书的统计数据发布和分析。

国际 SSL 证书的统计数据全部来自谷歌证书透明日志系统，数据真实有保证，因为每一张国际 SSL 证书都必须到谷歌证书透明日志系统备案才被信任，而这些数据都是公开可以查询的，这就是上面的所有统计数据的可靠来源。但是，我国还没有建立国密证书透明体系，零信技术 11 月 8 日在乌镇 2022 世界大会发布的全球首个国密证书透明日志系统已于 11 月 3 日正式上线提供国密 SSL 证书透明日志服务。但是，目前只有证签技术和零信技术签发的国密 SSL 证书提交到了国密证书透明日志系统中，其他已经签发国密 SSL 证书的 CA 机构由于需要时间改造现有国密 CA 系统以支持国密证书透明，目前还没有提交到国密证书透明日志系统中，所以也无法获得各家 CA 机构签发的国密 SSL 证书的真实数量。

本次报告仅能提供国密证书透明日志系统(sm2ct.cn)提供的国密 SSL 证书数据和我们平时收集到的一些数据，我国的国密 SSL 证书申请量为 **1000** 张，其中国密证书透明日志中的数据是 541 张，估计其他 CA 机构签发的国密 SSL 证书数量为 459 张。此数据只有象征意义，2023 年 Q1 报告计划发布由零信浏览器信任的 10 家 CA 机构各家通报的国密 SSL 证书数量，再加上国密证书透明日志中数据，下次的国密 SSL 证书的数量应该将是一个可信的数据。

目前，零信浏览器信任的国密根证书除了国家根和自家根外，CA 机构有：贵州 CA、数安时代、亚数信息、上海 CA、中金认证、天威诚信、沃通 CA、陕西 CA、网证通 CA 和四川 CA，希望各家 CA 机构能尽快完成对接零信国密证书透明日志系统，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。

五、 统计数据亮点和问题分析

1. 关于全站 https 加密

同上次统计数据相比，这次的数据中有 **23** 个省政府网站启用了 https 加密，上次的数据是 **22** 个，增长了 **1** 个，也就是启用 https 加密的比例已经达到 **74%**。但是，这些已经启用 https 加密的网站中仍然有部分网站支持不加密的 http 明文方式访问，仍然不能自动跳转到 https 加密方式访问，这使得部署的 SSL 证书并没有自动起到加密保护的作用，这个值得改进。

政务网站实现全站 https 加密非常重要，即使是仅发布向公众公开的信息的政府网站，即使这些网站没有用户登录页面，也需要部署 SSL 证书实现全站 https 加密。因为这些网站一定有链接到需要登录的政务服务网，这些有链接的页面如果没有使用 https 加密，则非常容易在传输的过程中被非法篡改而从可信的政府网站链接到了假冒的政府网站，从而导致用户在真正的政务网站系统的用户名和密码泄露，继而危害“一网通办”网站的系统安全。也就是说，所有政务网站无论是国家政务服务平台还是各个省级政务服务平台，还是各个局委办的政府网站，都必须是 https 加密方式运行，所有政务网站都加密了才能保证统一提供政务服务网站系统的安全。

2. 关于政府网站部署的 SSL 证书类型

我们检索了美国政府网站专属域名*.gov 的 SSL 证书申请量为 **3295** 张，英国政府网站专属域名*.gov.uk 的 SSL 证书申请量为 **3535** 张。同时，我们统计了这些政府网站所申请的 SSL 证书中的仅验证网站域名的 DV SSL 证书的占比，美国为 **50.83%**，英国为 **70.35%**，中国为 **80.28%**，而全球总的占比是 **83.81%**。

我们认为：对于国际 SSL 证书，我国政府网站**应该只是**申请 DV SSL 证书用于兼容所有浏览器实现 https 加密，没有必要申请需要提供身份认证材料的国际 OV SSL 证书和国际 EV SSL 证书，一方面的确很多政府单位是提供不了身份证明材料，另一方面是除了零信浏览器外的其他浏览器都不再在地址栏显示证书中的单位名称，失去了 OV SSL 证书和 EV SSL 证书能证明网站身份的价值。也正是由于这两个原因导致了大量的政府网站的 OV SSL 证书和 EV SSL 证书中显示的单位名称为企业名称，这显然是非常错误的网站身份信息，不仅完全失去了 SSL

证书能证明网站身份的作用，而且还有可能误导网站访问者。也正是这些原因，我们才认为我国政府网站的国际 SSL 证书应该只申请仅用于加密的 DV SSL 证书。

那么，政府网站的可信身份如何证明呢？当然，第一是专用的域名后缀标识(.gov.cn)，第二是我国政府网站都有“党政机关”认证标识。虽然这样的标识假冒政府网站也可以复制，但是只要网站访问者仔细查看认证信息应该还是能识别出假冒的认证标识的网站的。第三是零信浏览器已经推出的网站可信认证标识，由浏览器来完成网站身份认证和在地址栏展示网站可信身份，这是一个不可假冒的解决方案。

当然，还有一个传统的解决方案就是网站部署国密 OV SSL 证书和国密 EV SSL 证书，国密 SSL 证书由国内 CA 机构签发，可以采用各种灵活的身份认证方式来验证网站的真实身份，其实是不需要政府网站提供什么身份证明材料的。所以，对于国密 SSL 证书，我们推荐政府网站申请国密 OV SSL 证书和国密 EV SSL 证书，零信浏览器能在地址栏展示部署了这两类证书的网站可信身份。

3. 关于政务网站 SSL 证书到底应该由谁签发

本次统计中，我们发现了一个很值得单独列出的话题，中国台湾省政府网站申请了 3802 张 SSL 证书，其中有 3642 张 SSL 证书由政府专用顶级根证书或定制的专用中级根证书签发，占比高达 **95.79%**。我们还发现香港特别行政区的政府网站申请的 2103 张 SSL 证书中有 1489 张是由政府 CA-香港邮政 CA 签发的，比例也高达 **70.80%**。为什么这么做？当然是为了政务网站安全可控。如果政府网站部署的 SSL 证书是从特定的政务专用中级根证书签发的，则政务系统就可以增加一个更好的安全控制--政务网站系统只信任政务专用中级根证书签发的 SSL 证书，能简单有效地防止其他 CA 机构的 SSL 证书的错误签发和恶意签发，有效解决证书透明日志系统无法解决的证书自身安全问题，能有效阻止 SSL 中间人攻击。

我们认为：这个也值得大陆政府网站参考学习，我国正在不断改进营商环境，已经基本上 做到了所有政务服务都可以网上办和掌上办，但是便利服务的同时增加了政务系统的安全风险。 除了加强各种传统安全防护措施外，保障用于政务信息传输加密的 SSL 证书的自身安全非常 重要，唯一可靠解决方案就是所有政务网站所需的 SSL 证书都从定制的政务专用的中级根证 书签发，实现 SSL 证书本身的基础安全自主可控。当然，包括国际 SSL 证书和国密 SSL 证书， 用于双算法双 SSL 证书部署。

4. 关于为何这么多政府网站还没有部署 SSL 证书的思考

从 2022 年 4 个季度的报告数据可以看出，无论是从证书数量来看，还是同欧美政府网站的部署量来对比，目前我国政府网站的 SSL 证书部署量还是非常低的，这不利于政务“一网通办”服务的稳定安全可靠运行。零信任安全研究院为此组织力量对十几省市的政务云平台相关主管做了一些问卷和当面的调查，发现了这么低的 SSL 证书部署量的真实原因，本期特发布并提出建议，供有关决策者参考。

这些政务云平台主管们当然都支持网站需要部署 SSL 证书，否则所有浏览器都会提示“不安全”。虽然有些主管认为网站只是一些供公众了解的公共信息，没有必要加密。但是，真正的原因是现有正在提供政务服务的服务器系统不能随便动！不敢因为部署 SSL 证书实现 https 加密而有可能影响目前系统的正常运行，宁可没有部署 SSL 证书也要保证现有系统可靠正常运行。这是第一要务，部署 SSL 证书和部署国密 SSL 证书的合规要求变成了第二要务。更不用提，要支持国密 https 加密，Web 服务器软件都需要升级系统支持国密算法，那更是难上加难，不敢冒这个风险去改动现有服务器系统。

也就是说，大家都知道政务系统需要支持 https 加密、需要支持国密 https 加密，但是，目前的困境是安装 SSL 证书，实现国密改造有可能会影响现有的没有部署 SSL 证书的系统的可靠运行，这是万万不能接受的。政务云平台急需是零改造的、零改动现有政务系统服务器的、可以无缝从 http 升级到国密 https 加密的解决方案。这是来自一线的真实需求，值得相关服务提供商思考如何解决政务云平台实现 https 加密的真实难题。

如果解决了这个技术难题，那绝对不是现在的状况，连续两个季度都只有一个江西省政府官网启用了国密 https 加密。当然，为了确保用户使用任何浏览器都能正常访问政府网站，必须部署双算法双 SSL 证书，实现自适应算法 https 加密。我们同时呼吁我国互联网用户尽快使用支持国密 SSL 证书的国产浏览器，以实现即使 RSA SSL 证书被非法吊销，由于实际上是国密 SSL 证书在起加密作用而不会有任何影响，确保了用户能可靠地访问政府网站和各种重要网站。

我们同时呼吁所有国密 SSL 证书，特别是用于政府网站的国密 SSL 证书，应该必须尽快支持国密证书透明，以确保能及时发现用于恶意攻击签发的国密 SSL 证书或者草率错误签发的国密 SSL 证书，从而保障国密 https 加密安全。

六、小结

本次报告增加了两个关键数据的发布：国际 SSL 证书提供商和国密 SSL 证书提供商的数据，因为供给质量决定了消费质量，同时思考了为何在供给充足，甚至国际 SSL 证书已经供给过剩的情况下，为何消费市场没有起来，总的原因当然是供给方没有提供能真正满足消费方的真实需求的产品和服务，期待市场供给方能早日提供切合市场需求的产品和服务，只有这样，https 加密和国密 https 加密才能真正得到普及应用，才能真正大力提升我国互联网的基础安全保障水平。

本次发布的报告是 2022 年的最后一期报告，在 2023 年的第一天发布，零信任安全研究院感谢广大读者在过去一年对本报告的支持和信任，此报告由原先的 CEO 博客方式发布改为现在的由专职团队撰写发布，希望 2023 年我们能给广大读者带来更多的有价值的数据和信息。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，国际算法 SSL 证书市场被国外 CA 牢牢控制这已成为现实而无法超越，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！

“路虽远行则将至，事虽难做则必成”。祝福密码人，祝福祖国！

零信任安全研究院

2023 年 1 月 1 日于深圳

请关注零信任安全研究院公众号，实时推送精彩文章。