

中国 SSL 证书市场发展趋势分析简报-2025Q3

2025 年 10 月 9 日

本报告由**零信密码应用研究院**和**零信浏览器**全球独家联合发布，电子版首发渠道为零信密码应用研究院微信公众号：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))。

从本期开始改为每双季度发布一次前两个季度的 SSL 证书市场发展趋势分析报告，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 签发的国际 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和产业发展政策。

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**2025 年 9 月 30 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**13.7186** 亿张，比第一季度增加了**24.19%**。

排名前十五大 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 1 所示，第 1 位仍然是 Let's Encrypt，并且比一季度增加了 26.50%，市场占比比上季度有上升，第 2 位是谷歌，占比比上一季度略有下降，GoDaddy 排名第 3，环比增长接近 40%。值得一提的是，亚马逊从 Q1 的第 6 位上升到第 4 位，意味着其相关云服务由于 SSL 证书自动化带动了快速增长，环比增长高达 71%，这非常值得我国所有云服务商学习借鉴。传统 CA 机构 DigiCert 虽然保持第 5 位不变，但环比减少了 4%；而 Sectigo 则是下降了一位，由第 7 位下降到第 8 位，应该与 Sectigo 停止签发免费 90 天证书的有关。而 CDN 服务提供商 Cloudflare 有 130% 的增长，这个从未有的快速增长幅度估计与其从 3 月份开始默认免费支持后量子密码有关，即使其部分用户自动化配置是 LE 和 GTS 的 SSL 证书。还有一个上升两位的是 ZeroSSL，环比增加 246%，其竞争优势是多通道自动化签发 SSL 证书。最值得关注的是亚数信息，连续 5 个季度大幅度的下降(21%)，这应该与根 CA 不再提供免费 90 天证书和收费证书涨价有关。

排名	公司名称	签发量	占比%	环比%	Q1排名	公司类型	国别
1	Let's Encrypt	672,991,465	49.06%	26.50%	1	互联网软件	美国
2	谷歌	191,866,650	13.99%	18.94%	2	互联网公司	美国
3	GoDaddy	149,877,403	10.93%	39.70%	3	互联网公司	美国
4	亚马逊	83,019,038	6.05%	71.25%	6	云服务提供商	美国
5	DigiCert	82,421,634	6.01%	-4.14%	5	CA机构	美国
6	微软	54,138,320	3.95%	-41.10%	4	云服务提供商	美国
7	ZeroSSL	48,676,761	3.55%	246.45%	9	SSL证书提供商	奥地利
8	Sectigo	36,794,388	2.68%	3.75%	7	CA机构	美国
9	Cloudflare	34,415,822	2.51%	129.83%	8	CDN服务提供商	美国
10	IdenTrust	6,630,245	0.48%	80.13%	10	CA机构	美国
11	思科	2,866,397	0.21%	50.38%	11	网络设备制造商	美国
12	GlobalSign	1,515,030	0.11%	10.99%	12	CA机构	日本
13	Actalis	1,334,340	0.10%	59.40%	14	CA机构	意大利
14	cPanel	638,385	0.05%	-36.97%	13	软件提供商	美国
15	亚数信息	583,631	0.04%	-21.02%	15	SSL证书提供商	中国
16	其他	4,092,403	0.30%	11.44%			
	合计	1,371,861,912		24.19%			2025Q3

表 1

本期继续直接采用表格形式列出全球前 15 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 15 大中美不仅占据前 8 大，而且共有 11 家，占比 73%，证书签发量占 95.91%。统计表格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，并且拥有自己顶级根的 CA 机构。还有互联网公司、云服务提供商、设备制造商、网安公司)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。

如下图 1 所示，用圆饼图直观展示全球前 15 大 SSL 证书提供商的证书签发量排名和占比情况。

全球SSL证书提供商签发量占比图(2025Q3)

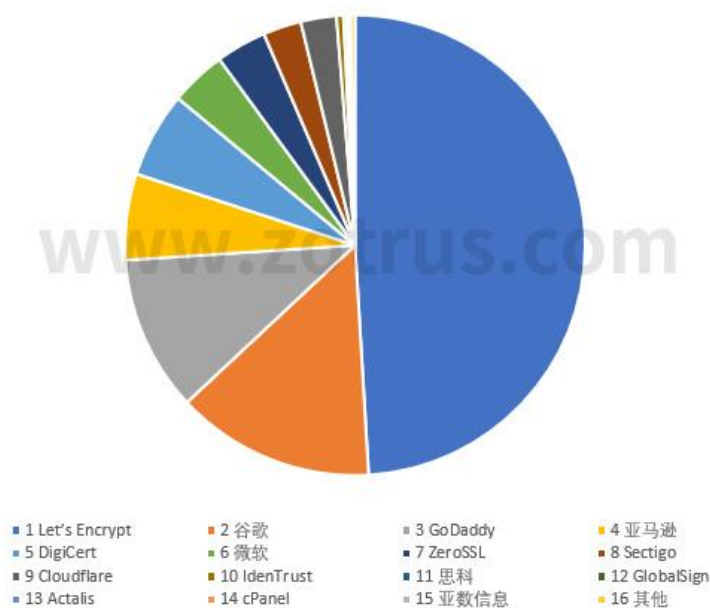


图 1

二、我国政府网站的 SSL 证书统计分析

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 2 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 1874 张，比一季度增长了 14.76%，这是在连续 3 个季度减少后的两位数增长，并且也只有 4 个省市自治区在减少，这也是首次，其他省市都有增长，其中增长幅度超过 60%的有三个省：山西省、西藏自治区和黑龙江省。排名前 7 位没有变化，排名上升最多的是天津市，上升了 5 位(从第 13 升到第 8)，黑龙江省也是上升了 5 位(从第 21 升到第 16)。

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
1	上海市	245	-0.41%	shanghai.gov.cn, sh.gov.cn	是	否	
2	浙江省	151	10.22%	zj.gov.cn	是	否	
3	北京市	133	14.66%	beijing.gov.cn	是	否	有
4	海南省	113	5.61%	hainan.gov.cn	是	是	
5	广西壮族自治区	108	35.00%	gxzf.gov.cn	否	否	
6	宁夏回族自治区	78	6.85%	nx.gov.cn	是	否	有
7	广东省	75	8.70%	gd.gov.cn	否	否	
8	天津市	73	37.74%	tj.gov.cn	是	否	有
9	山东省	71	10.94%	shandong.gov.cn, sd.gov.cn	否	否	
10	河南省	68	21.43%	henan.gov.cn	是	否	
11	陕西省	66	22.22%	shaanxi.gov.cn	是	是	
12	贵州省	63	40.00%	guizhou.gov.cn	是	否	
13	云南省	61	5.17%	yn.gov.cn	是	否	
14	吉林省	55	30.95%	jl.gov.cn	否	否	
15	江西省	52	23.81%	jiangxi.gov.cn	否	是	
16	黑龙江省	51	64.52%	hlj.gov.cn	是	否	有
17	甘肃省	50	-7.41%	gansu.gov.cn	是	否	
18	青海省	46	43.75%	qinghai.gov.cn	否	否	
19	湖南省	40	5.26%	hunan.gov.cn	是	是	
20	安徽省	39	0.00%	ah.gov.cn	是	是	有
21	重庆市	39	5.41%	cq.gov.cn	否	否	
22	河北省	34	47.83%	hebei.gov.cn	否	否	
23	辽宁省	31	10.71%	ln.gov.cn	是	否	
24	西藏自治区	29	70.59%	xizang.gov.cn	否	否	
25	新疆维吾尔自治区	28	-3.45%	xinjiang.gov.cn	是	否	
26	江苏省	22	4.76%	jiangsu.gov.cn, js.gov.cn	否	否	
27	福建省	19	26.67%	fujian.gov.cn, fj.gov.cn	否	否	
28	山西省	18	80.00%	shanxi.gov.cn	否	否	
29	内蒙古自治区	11	22.22%	nmg.gov.cn	是	否	
30	湖北省	3	-40.00%	hubei.gov.cn	否	否	
31	四川省	2	-33.33%	sc.gov.cn	是	否	
	合计	1874	14.76%		18	5	5

表 2

对于国密算法 SSL 证书的部署情况，31 个省市自治区省级政府官网中部署了国密 SSL 证书的有 5 个省：海南省、陕西省、江西省、湖南省、安徽省。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，只有 18 个省政府官网自动启用 HTTPS 加密，虽然有更多的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 5 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。

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

我们同时检索了*.gov.cn 的 SSL 证书申请量为 16507 张，比一季度增长了 11.11%。为政府网站*.gov.cn 签发 SSL 证书的 SSL 证书提供商前 18 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。对比上一期数据可以看出：亚数信息下降了 26%，天威诚信增长了 253%，CFCA、上海 CA 和沃通 CA 也都有两位数的增长，可以看出政府用户更加青睐国内 CA。免费自动化 SSL 证书提供商 LE 从一季度的第三位上升到第二位，这个数据值得注意，证书自动化已经开始在市县级政府网站实施。

排名	公司简称	证书数	占比	增长%	国别	根CA (国别)
1	DigiCert	5154	31.22%	7.76%	美国	DigiCert (美国)
2	Let's Encrypt	1412	8.55%	-9.89%	美国	ISRG (美国)
3	沃通CA	1275	7.72%	26.24%	中国	Sectigo/DigiCert/Assecods (美国/波兰)
4	亚数信息	1176	7.12%	-25.99%	中国	Sectigo/DigiCert (美国)
5	中金认证	1113	6.74%	20.19%	中国	CFCA (中国)
6	北京信查查	1092	6.62%	25.37%	中国	Assecods/Sectigo (波兰/美国)
7	上海CA	891	5.40%	26.56%	中国	Assecods x UniTrust (中国)
8	天威诚信	650	3.94%	253.26%	中国	Assecods (波兰)
9	Sectigo	576	3.49%	6.08%	美国	Sectigo (美国)
10	上海锐成	485	2.94%	-10.68%	中国	Sectigo (美国)
11	数安时代	455	2.76%	-8.82%	中国	Assecods/GDCA (波兰/中国)
12	GlobalSign	448	2.71%	8.21%	日本	GlobalSign (日本)
13	合肥网盾	398	2.41%	87.74%	中国	Sectigo/UniTrust/Assecods (美国/中国/波兰)
14	ZeroSSL	233	1.41%	-22.07%	奥地利	Sectigo (美国)
15	新网数码	182	1.10%	-10.78%	中国	Sectigo (美国)/UniTrust (中国)
16	腾讯云	165	1.00%	38.66%	中国	Sectigo (美国)
17	Assecods	158	0.96%	159.02%	波兰	Assecods (波兰)
	其他	644	3.90%	106.41%		国外CA
合计		16,507		11.11%		2025Q3

表 3

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。

政府网站国际SSL证书提供商占比图(2025Q3)

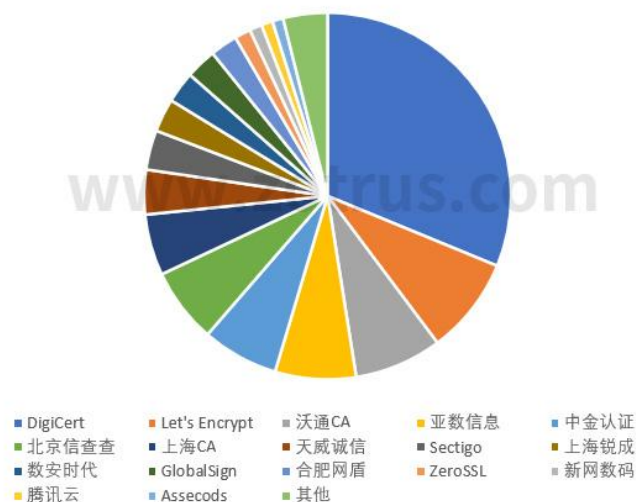


图 3

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 **16507** 张，台湾省的证书申请量增长 106%，估计与中华电信 CA 被谷歌浏览器不信任有关，大量网站需要重新从其他 CA 申请新证书。

	数量	增长%	检索域名	默认https	启用国密	WAF防护
中国大陆	16,507	11.11%	*.gov.cn	是	否	有
中国台湾省	31,001	106.14%	*.gov.tw	是	否	
中国香港特别行政区	2,286	-13.96%	*.gov.hk	是	否	
中国澳门特别行政区	503	8.17%	*.gov.mo	是	否	

表 4

三、 我国本土国际 SSL 证书提供商的统计分析

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 3 家是 CA 机构，仅排名为第五、第七和第十，其余都是全球知名的互联网巨头和云服务提供商。

如下表 5 所示，本次列入统计的本土 SSL 证书提供商有 16 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 16 家 SSL 证书提供商中有 6 家公司是 CA 机构，有 3 家是知名的云服务提供商，其他 7 家是商业公司。

而这 16 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。其他 13 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 16 家国际 SSL 证书提供商签发的有效证书数合计为 **84.6662** 万张，比一季度下降了 **11.78%**，这是连续 4 个季度都在下降，对比全球数据增加了 **24%**，只能说明国内 SSL 证书提供商输在了证书自动化管理上。本期虽然总数有下降，但是有 9 家机构的增幅超过两位数。对比一季度数据，亚数虽然还保持第一位，但是连续 5 个季度两位数的负增长，本季度跌破 60 万张，排名第二上海瑞成负增长 44%，其原因是根 CA-Sectigo 已经不再提供免费 90 天 SSL 证

书。新网数码增长 277%，上升了两位，上海环度增长 148%，排名上升了 4 位，中金认证下降了 1 位。

排名	公司简称	签发量	增长%	占比%	根CA (国别)
1	亚数信息	594,342	-19.68%	70.20%	Sectigo/DigiCert (美国)
2	上海锐成	54,237	-44.40%	6.41%	Sectigo (美国)
3	沃通CA	54,177	43.36%	6.40%	Sectigo/DigiCert/Assecods (美国/波兰)
4	新网数码	40,254	276.59%	4.75%	Sectigo (美国)/UniTrust (中国)
5	北京信查查	31,380	30.97%	3.71%	Assecods/Sectigo (波兰/美国)
6	合肥网盾	16,240	44.60%	1.92%	Sectigo/UniTrust/Assecods (美国/中国/波兰)
7	腾讯云	14,473	43.16%	1.71%	Sectigo (美国)
8	上海CA	8,063	26.90%	0.95%	Assecods x UniTrust (中国)
9	上海环度	6,284	147.69%	0.74%	UniTrust (中国)
10	阿里云	5,766	41.81%	0.68%	GlobalSign (日本)
11	天威诚信	5,534	20.80%	0.65%	Assecods (波兰)
12	中金认证	5,443	19.02%	0.64%	CFCA (中国)
13	广东堡塔	3,151		0.37%	Assecods (波兰)
14	浙江葫芦娃	1,792	0.79%	0.21%	Sectigo (美国)
15	数安时代	1,269	3.59%	0.15%	Assecods/GDCA (波兰/中国)
16	厦门纳网	865		0.10%	Sectigo (美国)
	其他	3,392	4.27%	0.40%	
合计		846,662	-11.78%		2025Q3

表 5

四、 我国国密 SSL 证书提供商的统计分析

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 **96462** 张，比一季度增长了 **154%**，本季度第一次实现了 3 位数的增长，并且是连续 12 个季度持续快速增长，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，增长最多的是政务系统用国密 SSL 证书。

本季度无新增 CA 机构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 5 家 CA 机构签发的国密 SSL 证书支持国密证书透明标准草案，本报告将像国际 SSL 证书一样列表排名各个商密 SSL 证书提供商签发的商密 SSL 证书，以帮助用户在选购商密 SSL 证书时优先选择支持国密证书透明的商密 SSL 证书提供商，从而保障用户自身的合法权益和网站安全。证书透明，向全世界告白-这张证书是我签发的，能大大提升 SSL 证书提供商的品牌知名度！

我们希望有更多机构，包括国家相关管理部门，能提供更加权威的国密证书透明日志服务。只有所有 CA 机构签发的商密 SSL 证书都像国际 SSL 证书一样都提交到证书透明日志系统，

商密 SSL 证书的签发统计数据才是真实的数据，商密 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、 本期关注点

1. 后量子密码(PQC)HTTPS 加密

美英法政府网站、美欧网银系统、美欧大学官网、全球前八大互联网流量网站在 Q2 和 Q2 纷纷启用后量子密码算法混合协议实现 HTTPS 加密，这是一个本季度发生的密码行业和网络安全行业的大事，意味着后量子密码从理论课题研究迈入了规模化部署阶段，这个规模化的部署使得全球互联网流量中已有 **41%**流量实现了后量子密码 HTTPS 加密，这些流量是抗量子攻击的真正安全的流量。这是一场无声的技术革命，非常值得我国密码业界和网络安全业界，以及政府主管部门高度重视和深入研究对策。

美欧互联网之所以这么迅速地实现后量子密码 HTTPS 加密，是因为目前已经存在“先收集后解密”的安全威胁，也就是先把由传统密码算法(RSA/ECC/SM2)实现的 HTTPS 加密流量收集保存起来，一旦量子计算机可用时就可以解密这些加密流量，使得现在的所有机密信息将都成为明文，这将是不可承受的最大互联网安全威胁。所以，美欧迅速行动起来采用后量子密码算法保护其机密信息安全。而我国到目前为止，没有一个政府网站和政务系统、没有一个银行网银系统、没有一所大学官网、没有一个互联网大流量网站实现了后量子密码 HTTPS 加密，这非常值得反思和赶紧行动起来。

零信密码应用研究院随机抽查了英国 100 个政府网站(*.gov.uk)，有 **38%**的网站已经实现了后量子密码 HTTPS 加密，其实现方式主要有两种方式：一是由政务云专用 CDN+WAF 服务统一提供支持，二是使用商业云服务提供商提供的 CND/WAF 服务实现。这两种实现方式都非常值得我国政务云服务和商业云服务学习与借鉴。

后量子密码是一场“输不起的竞赛”，我国关键信息基础设施系统每延迟一天启用 PQC，就多一天机密数据将来被解密的风险，所有现在已用传统密码算法加密的机密数据将来都会成为明文数据，这可能是灾难性的巨大风险。即便现在已完成全部系统商用密码改造，但传统密码算法（包括 SM2）不仅仅是在量子时代不安全，现在就已经存在数据安全威胁。所以，后量子密码迁移的实际紧迫性远超当前广泛开展的商用密码改造，我国应高度重视并加速推进后量子密码迁移工作，其优先级甚至应高于传统商用密码改造。最优策略是将两类密码算法改造同步完成。

2. DV SSL 证书已成为默认证书类型

熟悉本报告的读者也许已经注意到本期报告不再分别统计各类统计数据中的 DV SSL 证书、OV SSL 证书和 EV SSL 证书的数量和占比，这是因为全球 SSL 证书中的 DV SSL 证书占比已经超过 95%，DV SSL 证书已经成为默认证书类型。

这就好比 SSL 证书在 1994 年发明时只有 OV SSL 证书一样，现在 SSL 证书也很快基本上都是 DV SSL 证书了，所以，本报告从本期开始不再区分 SSL 证书类型，默认认为 SSL 证书就是 DV SSL 证书。这不仅是证书自动化时代的发展趋势，也是实现“密码敏捷”的需要，更是全球互联网向后量子密码迁移的需要。

零信密码应用研究院 和 零信浏览器 联合发布

2025 年 10 月 9 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 231 篇(共 69 万 2 千多字)和英文 99 篇(13 万 4 千多单词)。

