国内 CA 机构签发国际 SSL 证书的能力调研报告

2024 年 5 月 6 日

本报告由**零信浏览器**和**零信任安全研究院**全球独家联合发布，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))。

目前，国内用户特别是政府用户都倾向于选择国内 CA 机构签发的国际 SSL 证书，以满足身份数据不出境的相关要求。那么，国内有哪些 CA 机构有能力签发全球信任的国际 SSL 证书呢？这些 SSL 证书是否能满足用户的 HTTPS 加密应用需求呢？国内 CA 机构和国内 SSL 证书提供商如何抓住商密改造的大好机遇尽快占领 SSL 证书市场呢？零信浏览器和零信任安全研究院作为一个中立第三方首次联合发布了本调研报告，为政府机构和国内用户选购国际 SSL 证书提供参考。

本报告中的 CA 机构仅指国内 CA 机构，本报告中 SSL 证书提供商仅指 SSL 证书签发中级根 C 字段为 CN(中国)的全球信任的国际 SSL 证书提供商，本报告中的国际 SSL 证书指国际四大浏览器信任的国际算法(RSA/ECC)SSL 证书，而商密 SSL 证书是指国内商密浏览器(如：零信浏览器)信任的商密算法(SM2)SSL 证书。

一、 国内 CA 机构的国际 SSL 证书签发情况

目前已经完成微软 Edge 浏览器和 Windows 操作系统、谷歌 Chrome 浏览器和安卓操作系统、Mozilla 火狐浏览器、苹果 Safari 浏览器和 iOS 操作系统等四大主流浏览器根证书预置的国内 CA 机构只有 3 家：中金认证(CFCA)、上海 CA、数安时代(GDCA)，截止到 2024 年 5 月 3 日，这 3 家 CA 机构签发的有效 DV SSL 证书、OV SSL 证书和 EV SSL 证书数量如下表 1 所示，这些数据来自谷歌证书透明日志系统，真实可信。其中，OEM SSL 指 CA 机构为 SSL 证书提供商定制的 SSL 中级根证书签发的 SSL 证书，包括 DV/OV/EV SSL 证书，虽然这些 SSL 证书数量在 SSL 证书季度报告中未列入 CA 机构的统计数据中，但本报告列入是因为所有 SSL 证书的最终签发权和责任都是根 CA 机构。

排名	CA简称	DV SSL	OV SSL	EV SSL	OEM SSL	合计
1	中金认证	0	5808	789	0	6597
2	上海CA	1373	3787	20	937	6117
3	数安时代	52	317	9	0	378
	合计	1425	9912	818	937	**13092**
	占比	10.88%	75.71%	6.25%	7.16%	

表 1

中金认证只签发需要身份认证的 OV 和 EV SSL 证书，这一点值得点赞，因为 DV SSL 证书并没有网站身份信息，无法证明网站可信身份。而上海 CA 已经开始学习国际 CA 机构为国内 SSL 证书提供商定制 SSL 中级根证书，也值得点赞，因为只有这样，才能联合更多的有客户资源的非 CA 机构共同拓展 SSL 证书市场，从而实现快速占领市场。

而对于 SSL 证书类型，OV SSL 证书占比高达 76%，这完全同全球市场不一样，全球市场是 DV SSL 证书占比 87%，而 OV SSL 仅占比 13%。这个数据说明：目前国内 CA 机构主打市场是高端 OV SSL 证书，主打盈利能力，而不是低端的 DV SSL 证书市场(包括免费 SSL 证书)，这个定位也没有问题，值得肯定。

二、 国内 CA 机构的根证书预置信任情况

国际 SSL 证书是否可用，取决于根证书是否已经预置到四大浏览器信任，如果仅仅是一两个浏览器信任，还不具备使用价值。国内 CA 机构已经有 6 家通过 WebTrust 审计，并且申请了四大浏览器的根预置信任，这 6 家 CA 机构是：中金认证、上海 CA、数安时代、天威诚信、北京 CA、亚数信息，具体各家 CA 机构的根证书预置情况如下表 2 所示，表格最后一行列出了各大浏览器发布的可信根列表的最新时间或者最新版本号。其中，上海 CA 的苹果 Safari 浏览器和 Java 信任是通过与欧洲 CA 机构 Assecods 根证书做交叉签名实现，这是快速实现四大浏览器信任的方式，也是最大可能支持最老设备的有效技术手段。

	谷歌Chrome	微软Edge/Windows	苹果Safari/iOS	火狐浏览器	谷歌安卓	Java
中金认证	是	是	是	是	是	
上海CA	是	是	是*	是	是	是*
数安时代	是	是	是	是	是	
天威诚信	是			是	是	
北京CA				是	是	
亚数信息				是	是	
更新日期或版本	2024-03-12	2024-03-27	2024-01-31	2024-02-15	2024-03-06	V22.0.1

表 2

从表 2 可以看出，目前我国只有 3 家 CA 机构直接或间接完成了四大浏览器的根预置和信任，但是，这并不表明这 3 家 CA 签发的 SSL 证书的通用性是一样的，比如说：数安时代的根

在苹果 iOS 预置的版本是 12.1.3，在此之前的版本都是不信任的，如果用户不升级其 iOS 版本的话。对于 Windows 系统，由于微软采用了云端可信根下载模式，只要根已经预置信任，用户在第一次访问这个信任根签发的 SSL 证书时会自动下载可信根到 Windows 受信任的根证书存储处，所以 Windows 信任的根与预置时间先后没有太多关系，除非用户电脑不能联网。具体各家 CA 机构在四大浏览器的预置时间和支持的版本号，这里就不详细列出了，有兴趣的读者可以自己去查询或者咨询相关 CA 机构。

简单来讲，由于上海 CA 有欧洲 CA 的 2008 年老根做交叉签名，其签发的国际 SSL 证书的通用性更好。而中金认证的根证书已于 2016 年完成四大浏览器的预置信任，到现在已有 8 年了，也算是老根了，再老的设备也该淘汰了。数安时代的根证书则是 2019 年完成的，到现在也有 5 年了，也已经基本上支持各种常用设备了。用户可根据自己的业务需要和喜爱，选用这 3 家 CA 机构和其定制的中级根证书的 SSL 证书提供商签发的国际 SSL 证书。

三、 国内 CA 机构和 SSL 证书提供商应如何抓住商密改造的大机遇？

目前国内 CA 机构的国际 SSL 证书市场份额很低，这是由于我国 SSL 证书市场起步晚，CA 机构起步时仅抓住了 USB Key 证书的市场机会，而忽视了正在悄悄快速发展的 SSL 证书市场。当然，还有一个主要原因是由于国际 SSL 证书的信任话语权掌握在美国四大浏览器厂商手中。所以，我国 SSL 证书市场除了 2016 年有短暂的 6 个月时间的国内 CA 机构市场份额超过国外CA机构外，截止到今年3月31日，我国CA机构的市场份额在政府市场仅占10.78%，而在整个中国市场的市场份额估计低于 5%。

但是，现在机会来了，不仅是政府、金融等关键信息基础设施系统都会优先选购国内 CA 机构签发的国际 SSL 证书，确保符合相关数据不出境的合规要求，而且更重要是这些重要信息系统必须完成商密改造，必须采用商密 SSL 证书实现 HTTPS 加密。而为了兼容不支持商密算法浏览器，必须部署双算法双 SSL 证书—商密 SSL 证书和国际 SSL 证书，这就是国内 CA 机构和 SSL 证书提供商的大好机会，通过合规强制必须部署商密 SSL 证书来配套提供国际 SSL 证书，从而实现商密 SSL 证书和国际 SSL 证书的双丰收。

也就是说，国内 CA 可以通过国外 CA 无法提供的商密 SSL 证书而赢得竞争优势，CA 机构和 SSL 证书提供商应该抓住这次黄金机会。通过分析证书透明日志数据发现，数安时代在安徽省取得非常好的成绩，不仅拿到了国际 SSL 证书的大量订单，而且同时实现了普及商密 HTTPS 加密到县级政府官网，一举两得实现了社会效益和经济效益双丰收，这里也为数安时代点赞。

可以说，现在国内 CA 机构又迎来了第二个高光时刻，把握好机会。但还需要继续在以下两点改进和提高：

第一：必须尽快实现所签发的商密 SSL 证书支持商密证书透明，切实保障商密 SSL 证书的自身安全可信。既然签发的国际 SSL 证书都已经支持国际证书透明，升级 CA 系统支持商密证书透明也不是一件难事，因为商密证书透明标准就是参考国际证书透明标准制定的，使用同一技术原理实现，只不过是采用了不同证书透明日志数据签名算法(SM2 算法)而已。

第二：必须尽快实现双算法 SSL 证书的自动化管理，因为商密 SSL 证书的部署更需要自动化，彻底解决商密改造难题。两大国际 CA 机构(DigiCert 和 Sectigo)就是由于比其他厂商在自动化方面起步晚，而从全球第一和第二位沦落到了第六和第七位。这值得国内 CA 机构警示和深思，必须尽快拥抱证书自动化，抓住机遇，保持领先优势，实现新的飞跃，实现国际 SSL 证书和商密 SSL 证书的双丰收。

对于没有或不计划设置自有国际算法可信根的 CA 机构，也应该充分认识到这个市场趋势，尽快同已经拥有国际根的国内 CA 机构合作，国际 SSL 证书采用定制自己品牌中级根证书模式，而商密 SSL 证书则改造 CA 系统自己签发，尽快为用户提供双算法双 SSL 证书，尽快为用户提供自动化证书管理，而不是仅销售国际 SSL 证书，用户需要的是自动化实现 HTTPS 加密，自动化实现商密合规和全球信任的 HTTPS 加密，只有适应了市场的需要才能赢得市场，实现国际 SSL 证书和商密 SSL 证书的双丰收。

而对于国内 SSL 证书提供商和云服务提供商，同样可以发挥自己的客户资源优势，同国内 CA 机构合作定制国际 SSL 中级根证书和商密 SSL 中级根证书，为用户自动化提供双算法双 SSL 证书，也是有可能实现超越 CA 机构取得市场领先地位的，全球 SSL 证书市场就是这样把传统 CA 机构超越的，排名第一位的是一个软件厂商，第二三四五位都是云服务提供商，关键在于是否充分认识到这个巨大的商机和及时把握商机。

总之，商密合规要求对于国内 CA 机构和国内 SSL 证书提供商来讲都是一个大机会，一个可以实现把已经丢失的市场给拿回来的机会，大家赶紧行动起来，赢得双 SSL 证书市场，为普及商用密码应用做贡献，早日实现普及应用商用密码保障我国网空安全。

零信浏览器
零信任安全研究院
2024 年 5 月 6 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 163 篇(共 43 万 6 千多字)和英文 65 篇(7 万 9 千多单词)。