

好一个深圳创新-双算法 SSL 证书招标的高标准指标

深圳快速崛起的主要因素之一是深圳的创新精神，这是一个已经渗透到每一个深圳人骨髓里的精神。本文就讲一讲深圳政府部门的又一个创新之举。

深圳市大数据资源管理中心 9 月份发布了“双算法 SSL 证书服务采购公告”，这个公告是一个朋友告诉笔者的，看完公告附件的采购需求，笔者做实吓了一跳，这绝对是创新哦，是在为以后全国各地的政务云平台采购 SSL 证书立下了一个默认的技术规范要求，一个非常好的模板。笔者今天就讲一讲这个标书的创新之处，主要有以下三大创新。



第一个创新：标题直接写“双算法 SSL 证书服务采购”

直接明确告诉供应商采购的是双算法 SSL 证书，而不是简单写 SSL 证书，或写采购国密 SSL 证书。网站部署双算法双 SSL 证书是一个既满足了国密合规又满足了全球信任的双需求的最佳方案，只有部署了双算法双 SSL 证书才能实现自适应算法 HTTPS 加密，国密浏览器采用国密算法实现 HTTPS 加密，不支持国密算法的浏览器采用国际算法实现 HTTPS 加密，因为政务系统是面向所有老百姓的，不能强制要求用户必须使用国密浏览器才能使用政务系统，方便老百姓使用任何浏览器都能访问政务系统。

目前我国的政务系统仅部署国际 SSL 证书是不合规的，但是仅部署国密 SSL 证书又存在浏览器的广泛支持问题，而同时部署国密 SSL 证书和国际 SSL 证书就解决了这个矛盾，既合规又实用，这应该是所有政府网站和政务系统的默认配置，当然这种配置是一个过渡时期的配置，一旦我国实现了国密 HTTPS 加密全生态产品的全面支持国密算法，就只需部署国密 SSL 证书了。

第二个创新：明确要求双 SSL 证书必须都支持证书透明

这个要求绝对是国内首创，以前绝对没有过。并且是在产品功能上占 25 分的高比例，为什么？因为只有证书透明才能保证签发给深圳政府域名的 SSL 证书是政务云平台管理员自愿申请并完成域名控制权验证的 SSL 证书，这才是有保障的 SSL 证书。如果不支持证书透明，无法保证 CA 机构不会恶意签发或者错误签发绑定深圳政府域名的 SSL 证书。

产品功能要求的原文是“国际算法 SSL 证书支持国际证书透明，国密算法 SSL 证书支持国密证书透明，双证书签发行为透明公示”，特别强调了双算法 SSL 证书签发行为的透明公示。由于谷歌从 2013 年开始强势推动国际证书透明，已经有超过 108 亿张全球信任的国际 SSL 证书实现了证书透明公示。但是，这个国际证书透明体系不支持国密 SSL 证书，而国密证书透明相关国密标准还在制定立项中，深圳政务云平台为了保障政务系统的国密 HTTPS 加密的安全，敢为天下先，全国率先在公开招标技术指标中明确要求必须支持国密证书透明，这不得不让笔者拍案叫好，这是来自国密 SSL 证书用户的刚需和强音，也必将一定会成为全国各省市政务云平台招标 SSL 证书的标准要求，因为只有国密 SSL 证书的透明签发才能保障国密 HTTPS 加密的安全。

笔者现在非常能理解为何谷歌在 2013 年那么强势地推动证书透明技术，因为谷歌自己就是各种恶意攻击签发或错误操作签发的 SSL 证书的受害者，不断有用于攻击的绑定 gmail.com 和 google.com 的 SSL 证书被签发，而这些 SSL 证书都是全球信任的 SSL 证书。所以，谷歌认为浏览器的信任列表不足以保障 SSL 证书用户的安全，必须还要有一个来自第三方的约束机制来约束 CA 的证书签发行为，这就发明了证书透明机制，并牵头制定了证书透明国际标准 RFC6962。经过 10 年的努力，截止到现在，每一张全球信任的国际 SSL 证书都支持证书透明，累计有超过 108 亿张国际 SSL 证书都已经实现了证书透明公示，以保障每一张国际 SSL 证书的安全可信。国密 SSL 证书当然也理当如此，所以，深圳政务云平台在招标时明确要求支持国际证书透明和国密证书透明。

第三个创新：明确要求免费配套提供不限用户数量的国密浏览器

这个要求是政府用户对目前市场上的收费的国密浏览器说“不”，因为自从有了互联网，有了浏览器，所有国际流行的浏览器都是完全免费的，为何支持国密算法的浏览器就要收费呢？这不是故意拿我们政府用户必须国密改造来卡我们脖子吗？这就是“趁火打劫”，是不正当的商业行为，深圳必须打击这种恶为！怎么打击？只能在招标 SSL 证书时明确提出来，立一个标杆，明确态度，SSL 证书提供商必须搞定免费配套提供国密浏览器这事。

笔者相信深圳政务云平台在起草标书时一定已经了解到市场上已经有了完全免费的国密

浏览器，所以才有底气敢叫这个板！这个叫板比笔者写文章呼唤有力量多了！笔者又是拍案叫绝！因为要想普及国密 HTTPS 加密，必须有完全免费的国密浏览器才能实现，这是我国普及国密 HTTPS 加密的大事，深圳政务云给了有力的推动，必须点赞！

除了以上三大创新外，标书对产品资质要求也非常合理和灵活。“国密 SSL 证书由具有工信部和国密局 CA 许可证的 CA 机构的国密根证书签发”，这个要求比“投标商必须是具有工信部和国密局 CA 许可证的 CA 机构”更宽泛和更公平，这样才会有更多的合格投标者参与，但也并没有降低国密 SSL 证书的签发标准和国密合规要求。这是一个非常高明的做法，既符合市场的公平公正和不故意抬高招标门槛的原则，又能保障产品质量和合规要求。

总之，笔者认为，这次深圳政务云平台的 SSL 证书招标就是一个大创新，具有国密 SSL 证书发展的里程碑意义，这就难怪一位国密局领导得知这个招标后说“为深圳点赞”。这个创新不仅能让国密 HTTPS 加密有力保障深圳政务云平台的 Web 系统的安全，而且给全国各省市政务云平台的 SSL 证书招标提供一个完美的范本，深圳继续在各个方面包括在商密应用方面起到了排头兵的带头示范作用，也必将进一步推动我国政务系统国密 HTTPS 加密应用的普及，从而有力保障我国政务系统安全。笔者也特撰文为深圳政务云平台点赞。

有诗为证：

深圳创新是基因，商密应用真带头。

证书透明很重要，率先要求双支持。

双密码算法证书，双透明日志保障。

浏览器支持国密，免费配套明要求。

标书公平又公正，国密合规和兼容。

政务证书要招标，深圳标书是范本。

点赞深圳里程碑，商密应用有创新。

商密加密必普及，网站安全有保障。

王高华

2023 年 10 月 17 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。

