CA 转型，势在必行，一定能行！

笔者作为从事了 CA 事业 17 年的老兵，虽然已经离开了沃通 CA，但是如同我的开篇博文所写，我会“不忘初心”继续在 CA 领域奋斗，以期完成未了的 CA 证书应用事业。周末整理以前的老照片，当看到下面这张照片时很有感触，这是 2013 年 11 月 26 日第一次参加每年举办的“中国电子认证服务产业联盟工作年会”，我很是怀念疫情之前每年能有机会同 CA 行业领导和 CA 同行汇报和交流学习的机会，可惜由于疫情这个会议已经停办了一年，也不知道今年是否续办。但是，笔者认为，同 CA 同行交流还是需要的，笔者就写篇博文同 CA 同行网上交流吧，不对之处敬请同行朋友们指正。

1. CA 转型，势在必行

大家都知道，政府为了简政放权，已经把企业必须使用 CA 证书的许多业务都不强制要求使用了，许多业务都可以使用微信或支付宝刷脸搞定。这对于 CA 业务来讲，绝对是一个非常大的危机，可以说这可能是一个决定 CA 机构生死存亡的危机，不得不引起各 CA 机构的高度重视。

所幸的是，笔者在 2019 年 4 月 15 日在深圳召开了“国密证书全生态应用战略研讨会”，有 26 家 CA 机构负责人积极参会，大家都在危机中看到了希望。而随后的 2019 年 10 月 26 日我国颁布了《密码法》，并于 2020 年 1 月 1 日正式生效。《密码法》讲得非常清楚，要解决网络安全问题，必须采用密码技术。而如何采用密码技术，第二条“本法所称密码，是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务”讲得非常清楚，这一定是 CA 机构的一个巨大的市场机会，就看大家是否能抓住了。

按照《密码法》对密码的定义，CA 机构不仅需要继续提供安全认证技术、产品和服务，这是目前 CA 机构的主营业务，必须继续加强这个方面的各种密码应用，使得各种政务信息系统能满足《密码法》的合规要求，而不能仅提供 CA 证书而被边缘化。而且更重要的是：CA 机构一定要加强《密码法》要求的第二项-“对信息进行加密保护”这个更大市场的投入，这是 CA 机构的最大的市场机会。

CA 机构转型的关键是抓住《密码法》的强制合规要求的市场机遇，为用户提供各种合规所需的密码产品和服务，特别是非传统 CA 业务的“信息加密”业务，这个转型非常重要，也必须尽快行动起来。

中华人民共和国密码法

第二条　本法所称密码，是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。

第二十七条　法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。

第二十九条　国家密码管理部门对采用商用密码技术从事电子政务电子认证服务的机构进行认定，会同有关部门负责政务活动中使用电子签名、数据电文的管理。

2. CA 转型，一定能行

要做好“信息加密”市场的转型，当然必须抓住 SSL 证书市场，这个市场本来就应该是 CA 机构的主营业务，只是由于历史原因而被 CA 机构忽视了，现在赶紧抓起来还不晚。笔者现在回想起 2019 年的“国密证书全生态应用战略研讨会”和随后的“国密证书全生态应用巡回培训”这两件大事，甚是欣慰，这是笔者现在看来最有价值的研讨会和最有价值的将近一个月的出差，

累计培训各 CA 机构的相关从业人员超过 300 人，为我国国密 SSL 证书的普及应用打下了一定的人才基础。

回到正题，正与我在开篇博文所讲，我要“不忘初心”，完成未了之证书应用事业，当然不能忘了曾经一起奋斗过的 CA 朋友们。所以，这次重新创业，我为自己定下来的第一个目标是帮助各个 CA 独立拿下 SSL 证书这个业务，SSL 证书是《密码法》中的“信息加密”的最典型和最广泛的应用，没有之一。所以，CA 要转型，就得从 SSL 证书业务开始，把握《密码法》机遇，把这个市场拿下。

当然，这也正是我能发挥自己的优势的地方，我已经充分发挥这 17 年来同国际 CA 机构负责人结下的友谊，低价批发了一批全球信任的定制中级根证书，可以让各家 CA 能快速拥有自己品牌的中级根证书，自己签发全球信任的 SSL 证书，这个是 SSL 证书业务必配的基础。

同时，我还会帮助各 CA 充分利用现有的 CA 系统来签发国密 SSL 证书，这个属于友情支持指导，能让各个 CA 稍微改造一下现有 CA 系统就能自主签发国产国密浏览器都信任的国密 SSL 证书，满足政务网站的国密 https 加密应用需求。

我在 2018 年 12 月 17 日-18 日的“**网络空间可信峰会**”上首次提出了双算法双 SSL 证书部署的解决方案，只有这样才能满足政务网站的 https 加密应用需求，因为仅部署 RSA SSL 证书，则无法满足国密合规的硬要求。但是，如果仅部署国密 SSL 证书，则必须强制要求用户使用支持国密 SSL 的浏览器，这个对于政务网站来讲视乎也做不到。所以，为了保护电子政务用户的机密信息和隐私信息安全，政务网站必须部署双 SSL 证书，部署全球信任的 RSA 证书只是为了满足支持所有浏览器的应用需求，毕竟国产浏览器还没有达到 100%普及的市场程度。而部署国密 SSL 证书则是为了满足政务网站的国密合规需求，可以在政务办公网内部全部使用国密浏览器实现国密 https 加密。

也就是说，我会发挥深耕 SSL 证书十七年的优势，真心帮助各个 CA 同时具有自主签发自主品牌的 RSA SSL 证书和国密 SSL 证书的能力，从而快速转型开拓 SSL 证书这个本应属于各 CA 的大市场，这个是有保障的，CA 转型，一定能行！

当然，《密码法》的“信息加密”不仅仅是 https 加密这一项，还有文档加密、邮件加密、数

据加密等各种用数字证书来实现信息加密保护，这需要各 CA 机构持续不断的创新，不断地提供满足用户国密合规的产品和服务，不断开拓新的业务和新的市场，从而实现华丽转型，为保障我国互联网安全、物联网安全和工业互联网安全做出 CA 机构应有的贡献，笔者愿继续同各个 CA 界朋友一同努力一同为之奋斗。

王高华

2021 年 12 月 9 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。