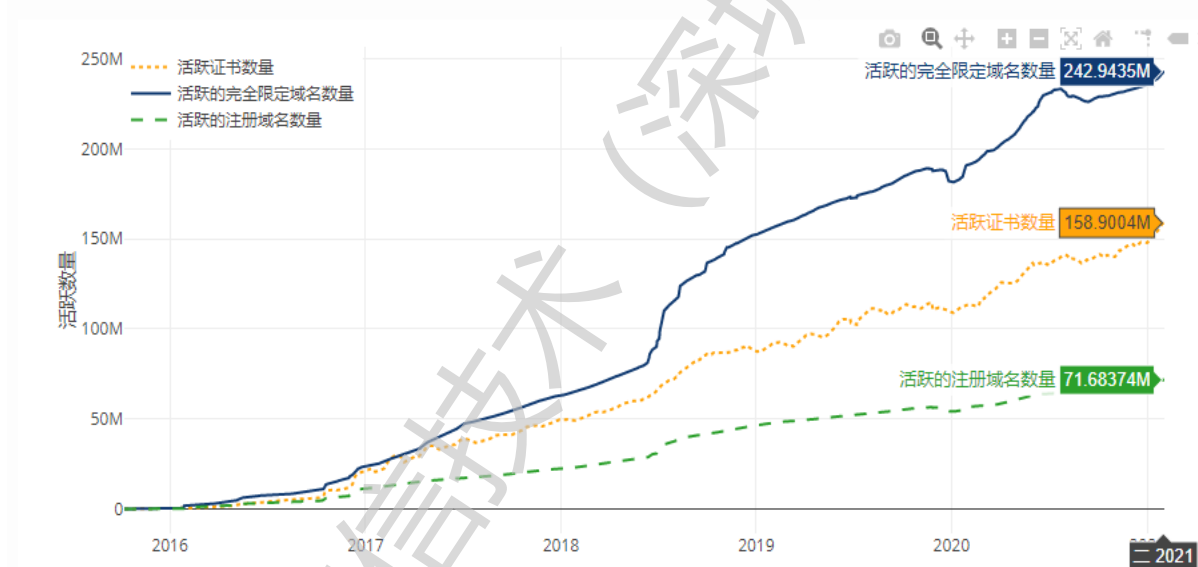


## 我们能从 Let's Encrypt 的成功学到什么？

(2021 年 2 月 22 日)

Let's Encrypt 大家应该已经都不陌生了，根据其官网的统计，活跃 SSL 证书数量接近 1.6 亿张，每日签发 SSL 证书最高达到 209 万张，2.42 亿个网站都在使用其 SSL 证书，全球市场份额超过 65%，这个成绩只用了 5 年时间。我们能从其获得的巨大成功学到什么？可能每个人都有自己的答案，我愿意在此同大家分享一下我的看法，供大家参考。

### Let's Encrypt 增长趋势



为了回答这个问题，这就要稍微了解一下 SSL 证书知识，以便没有经历过 SSL 证书申请和部署使用的用户参考。如果你了解这些，可以直接跳过到下一段落。SSL 证书用于网站 https 传输加密，因为 Web 超文本页面在发明使用时采用的是明文传输的 http 协议，从浏览器到服务器之间的信息传输就像现在的邮件传输一样也是明文传输的，这就容易泄露用户从浏览器提交的登录用户名和口令等各种机密信息，特别是互联网开始用于网上支付时，一旦支付信息在传输过程中被非法篡改和窃取，那就是大问题了，转账给张三的一万元就可能被篡改为转账给李四。所以，浏览器鼻祖 Netscape 公司就发明了 SSL 协议，在服务器上部署 SSL 证书，浏览器支持用证书公钥加密 http 流量，实现 https 传输加密，这个 S 就是 Secure (安全)的意思。简单地讲，要实现 Web 客户端到服务器端的传输加密，用户必须从第三方 CA 申请 SSL 证书，当然以前都是收费的，并且高端品牌的 SSL 证书在 2000 年时收费高达 8000 元/年，想想 20 年

前大家的工资收入就知道这意味着什么，意味着 SSL 证书不可能普及应用。不仅仅是费用高，而且从申请证书到拿到证书可能需要一周时间，拿到证书后还要非常费力地在各种 Web 服务器上部署使用，从而实现 https 加密传输，保护用户 Web 流量的数据安全。

各位如果看过我的博文[《饿了，你需要的是面包而不是面粉或小麦》](#)的话，可能还记得我讲的产品创新观点是：让我们回归用户需求的本源来分析用户的需求，为用户直接提供所需的产品，而不是各种中间产品。就 https 网站传输加密来讲，用户需要的是实现从浏览器到服务器之间的传输加密，而不是 SSL 证书。而目前全球 CA 都是在销售 SSL 证书，这是没有认清用户的真实需求是什么，但是领先的浏览器厂商 Mozilla (火狐浏览器)认识到了用户的真实需求，那就是 Web 传输加密。Mozilla 牵头联合其他单位一起推出了现在的 Let's Encrypt 服务，与其说这是一个 CA 项目，还不如说是一个软件项目，因为 Let's Encrypt 并不像其他 CA 机构一样让用户在其网站上申请 SSL 证书，把证书给用户让用户在服务器上去部署使用，而是开发了一个软件让用户部署在服务器上，启动此软件就能自动为用户网站配置好所需的 SSL 证书，从而自动实现 https 加密。

用户需要的就是 https 加密，不是 SSL 证书。所以，Let's Encrypt 没有给用户 SSL 证书，给用户一个软件，让此软件自动为用户申请 SSL 证书和自动部署证书实现 https 加密。现在，大家应该能理解为何 Let's Encrypt 能获得如此大的成功的秘诀和原因了。可能有些了解 CA 市场的读者会说，Let's Encrypt 的成功是因为证书免费，免费当然是一个因素之一，特别是推出新产品时，免费能吸引用户试用和使用，但是，这绝对不是一个重要的原因，重要的原因是其产品真正满足了用户的真实需求！我坚信，即使哪一天 Let's Encrypt 服务不再免费，这些用户也是愿意付费的，因为这些用户已经习惯了只需安装一个软件就什么也不用做的状态以后，让这些用户为了省钱再去向传统 CA 繁琐地申请证书和部署证书，那是不可能的，这些用户一定会选择付费继续使用 Let's Encrypt 服务。



这就是我对 Let's Encrypt 为何能取得成功的原因分析。如果你已经是密信 App 的用户，或者看过我的博文《[饿了，你需要的是面包而不是面粉或小麦](#)》，你会发现密信 App 也是采用了同样的“套路”哦！传统的邮件加密服务，用户需要向 CA 购买和申请邮件证书，拿到证书后需要在支持 S/MIME 邮件加密的邮件客户端软件中费力配置证书，费力同收件人交换公钥，才能实现邮件加密。而密信 App 直接集成了证书自动申请、证书自动配置使用和自动获得加密公钥的各种功能，让用户直接使用密信 App 就能实现邮件加密，而不用关心什么是邮件证书。这就不难解释为何密信 App 推出市场就得到了用户的热爱，现在用户已经覆盖了 171 个国家和地区。我们推出的我签文档服务也是这个思路，让用户可以不用关心文档签名证书，无需上传待签名文档到签名平台，直接使用我签文档 App 在用户电脑上实现全自动文档数字签名。



我们比较一下两者的异曲同工之处，都有一个云密码基础设施，用于为用户签发用户所需的证书及其他配套服务。都给用户一个客户端软件，由这个客户端软件负责繁琐的证书申请和证书部署工作，用户一次安装软件得到的是一劳永逸的数据加密和数字签名服务。笔者作为一个曾从事 CA 业务 15 年之久的从业者，现在跳出了 CA 圈而从软件开发圈的观点来重新认识 Let's Encrypt 的成功，并且已经把这个解决问题的思路成功应用到邮件加密和文档签名应用上。



但愿本文对 CA 从业者和软件开发商都能有所启发。当然，我也相信此文一定能帮助密信用户充分理解我们的产品优势，并与我们一同成长，共同实现“电子邮件全加密”和“电子文档全签名”的远大理想，共同努力提升全球互联网安全，让互联网更好地造福人类。

-----END-----



想联系我讨论此话题？请使用 [密信App](#) (  -  ) 扫码发加密邮件给我, 我一定会回复您的加密邮件。

© 2021 密信技术 (深圳) 有限公司