关于 Mozilla 对沃通 CA 系统安全事件调查的补充说明

(2016 年 9 月 23 日)

自从 8 月 24 日收到 Mozilla 邮件到现在已经一个月了，沃通回答了邮件组中大家提出的问题，并发布了两份调查报告(初步调查报告 和 最终调查报告)。

沃通已经认识到自己的错误并已经确认这些问题都得到修复和整改。沃通愿意接受在保证现有用户权益的前提下的可能发生的任何公平合理的制裁。

为此，沃通最后再补充说明以下 4 点：

1. **我们一直在不断进步和完善中。**

   根据已经发现的问题，2015 年签发 101485 张 SSL 证书，严重问题证书有 33 张，占比 0.03%，总的问题证书 1647 张，占比 1.623%。

   2016 年截至到 7 月 4 日签发 94073 张，没有出现严重问题证书，总的问题证书只有 12 张，占比 0.013%。

   从 2016 年 7 月 5 日起所有证书提交谷歌证书透明日志服务器后签发了大约 43000 张证书，没有发现任何有问题证书，错误率为 **0.000%**。

   从 **1.623%**到 **0.013%**再到现在的 **0.000%**，可以看出我们的系统一直在不断完善和改进。

2. **为何 2015 年有这么多的事件和这么高的错误率？**

   这是我们正在反省的问题，我们认为主要有两个原因：

   (1) **用户量快递增长**：2015 年 1 月 1 日我们向全球用户独家开放了 3 年有效期和绑定 100 个域名的免费 SSL 证书的申请，大受全球用户欢迎，每日订单量剧增，短短 3 个月时间用户已经覆盖全球超过 180 个国家和地区。一天只签发几张证书和一天签发上千张证书相比，在数量级上是千倍的快速增长，其中不乏有恶意攻击订单，这对系统的安全可靠是极大的挑战。这次的事件中的一些问题就是由于大量并发请求而导致数据库响应问题而出错。

   (2) **对国际标准研究不够**：鉴于国外公司对中国公司的技术封锁，沃通只能自主研发所有系统，包括 Buy 下单系统、CMS 后台证书管理系统、PKI/CA 证书签发系统、CRL/OCSP 证书吊销查询系统和 TSA 时间戳系统等，系统庞大并且都必须遵守所有相关的国际标准，我们并没有把所有标准研究透，导致部分系统出现了一些不符合国际标准的问题。

3. **为何 2016 年 7 月 5 日全部提交 CT Log server 后就不再出错了？**

   这有两个原因：

   (1) 系统经过了 2015 年的不断出现问题并不断的及时修复和完善，2016 年除了在 1 月 1 日前后的 SHA-1 到 SHA-2 的过渡期出现了一点小问题外，

基本上没有出现其他任何问题，证明所有系统已经稳定和可靠运行。目前，每月 CRL/OCSP 查询量已经高达 200 亿次。

(2) 我们认为证书透明是一种非常好的自律机制，能让 CA 员工可以高度重视证书产品质量；和他律机制，方便第三方监督 CA。
沃通是全球第一家**主动**把所有签发的 SSL 证书都全部发布到谷歌证书透明日志服务器上供全球用户查询的 CA，沃通此举的目的就是让广大用户放心使用沃通证书，希望能带动全球 CA 都能做到公开、透明的签发每一张证书，接受全球用户、浏览器厂商和相关利益方的全面监督，这将有益于全球互联网的安全。

4. 关于事件中有关使用国产加密算法 SM2 签发 SSL 证书的问题

我们认同这违反了相关国际标准(只能使用美国国家标准研究院(NIST)指定的 3 种椭圆曲线 NIST P-256、P-384 和 P-521)。但作为一个有中国牌照的 CA，我们必须遵守我国的有关法律法规，我们必须积极同国产浏览器厂商合作共同从事采用 SM2 加密算法签发全球信任的 SSL 证书的研究工作和相关实验。

沃通作为相关国际标准组织 CA/Browser Forum 的成员单位，将不遗余力地不断推动国产加密算法能够成为国际标准允许使用的加密算法。

最后，通过这将近两年时间的高签发量的磨练，沃通的系统已经更加安全可靠，沃通的客服队伍和鉴证队伍也已经更加成熟，我们有能力和决心为全球用户特别是中国用户提供更好的产品(包括支持中文)和更优质的服务，这也是我们对全球用户特别是中国用户的承诺。

沃通电子认证服务有限公司

2016 年 9 月 23 日