首次 IETF 之旅：不止于推动标准草案，更学到了许多

2026 年 3 月 23 日

在深圳举办的为期一周的国际互联网工程任务组织（IETF）第 125 届大会已于 3 月 20 日完美落幕。作为一位多次参与国际标准组织会议（如 CA/浏览器论坛）的密码从业者，这次是笔者首次以专题研讨会主持人的身份参与 IETF，感触尤为深刻。这次经历，于笔者而言确实是“一举两得”：既成功推动了笔者深度参与的商密混合 PQC 算法 RFC 草案的社区交流，更以一个“初学者”的视角，近距离观察和学习到了 IETF 这个全球顶级标准组织的运作精髓。以下是笔者的几点心得。

一、专题研讨会：推动“商密+后量子密码”混合算法成为国际标准

3 月 16 日上午，笔者成功主持了一场聚焦于“后量子密码迁移”的专题研讨会（Side Meeting）。核心议题是介绍并推动由我国密码团队主导的《TLS 1.3 商密混合 PQC 算法》RFC 草案。该草案旨在应对两大挑战：一是满足我国商用密码合规要求，二是应对未来量子计算对现有公钥密码体系的颠覆性威胁。我们提出的解决方案是将商密 SM2 算法与抗量子算法 ML-KEM-768 融合，形成一个新的混合密码套件。这个草案在此之前已经获得国际互联网号码分配机构（IANA）分配的 TLS 支持组算法编号 4590，为推动草案的标准化进程迈出了坚实的一步。同时，OpenSSL 开发团队在上个月已完成 Issue #1855 (支持 TLS 1.3 商密算法和商密混合 PQC 算法)的代码开发、审核和测试工作，预计不久的将来 OpenSSL 正式版本也会支持 SM2MLKEM768，这将为全球范围的生态支持又近了一大步。

草案能否成为标准，生态建设是试金石。研讨会重点展示了围绕 SM2MLKEM768 算法构建的全生态系统，证明了其技术的可行性与成熟度：

- **服务端**：由蚂蚁集团旗下的铜锁 SSL 密码中间件实现了全面开源支持。
- **客户端**：零信浏览器已同时支持 SM2MLKEM768 和 X9MLKEM，为用户提供“量子安全”的 HTTPS 加密连接。
- **企业端**：零信 HTTPS 加密自动化网关，为企业提供了便捷的、原 Web 服务器零改造的、支持证书自动化的后量子密码迁移解决方案。

令笔者备受鼓舞的是，**研讨会现场即有国际厂商代表明确表示，将尽快在其维护的 Java 平台开源密码库 Bouncy Castle 中支持 SM2MLKEM768，推动该算法在 Java 生态中落地。**这正是我们期望的——通过开放研讨，凝聚全球智慧，共同推动标准草案从中国走向世界，最终成为 IETF 的正式国际标准。

二、对我国制定行业标准和实施标准草案的启示

如果说第一部分是笔者作为“推动者”的收获，那么这一部分则是笔者作为“学习者”的感悟。IETF 的工作方式，本身就是一个巨大的学习样本。其核心工作是制定 RFC 国际标准，这些标准详细定义了互联网的技术基础，如寻址、路由和传输技术，以及 TLS 1.3、QUIC 和 WebRTC 等数十亿人日常使用的协议。RFC 原意是“征求意见稿”，如今已成为“定稿的国际标准”。其制定过程高度开放：任何人均可提交草案，所有人都能通过邮件列表、会议记录、线下会议等方式公开参与，所有参与者都是出于推动“让互联网更好”的使命而自愿工作。

这种开放模式催生了惊人的科技创新与普及速度。以目前已广泛使用的混合 PQC 算法 X25519MLKEM768 为例，它的发展时间线极具参考价值：

- **2024 年 8 月 13 日**：NIST 正式发布三项 PQC 标准，其中包括 FIPS 203（ML-KEM）。
- **2024 年 8 月底**：由来自 PQShield 和亚马逊云的两位专家提出 ECDHE 混合 MLKEM 个人 RFC 草案。
- **2024 年 11 月 12 日**：谷歌 Chrome 131 版本正式支持在 TLS 1.3 中使用 X25519MLKEM768。
- **2025 年 3 月初**：个人 RFC 草案被 IETF TLS 工作组认领。

- **2025 年 3 月 17 日**：Cloudflare 宣布为所有 CDN 用户免费升级支持该混合 PQC 算法实现 HTTPS 加密流量分发。
- **2025 年 4 月 8 日**：OpenSSL 3.5.0 原生支持该混合 PQC 算法。
- **2026 年 2 月**：正式批准为 Proposed Standard（拟定标准），历时仅一年半时间。

这个时间线中最值得深思的是，**当该标准草案最终成为国际标准时，全球已有超过 65%的互联网流量支持此算法。**这种"**标准未动，依据草案应用先行**"的生态驱动模式——即工程实现、巨头部署与标准制定同步推进——非常值得我国业界学习，特别是密码业界。

反观我们推动的 SM2MLKEM768 草案，本次研讨会重点展示的正是其从客户端、服务端到企业级的完整生态。国际厂商的积极回应也印证了这条路径的正确性。笔者热切希望，我国其他相关开源密码库能快速跟进支持，其他国产浏览器厂商和 SSL 网关厂商也能快速支持，正在制定或新制定的密码行业标准能尽快参考对齐此标准草案。笔者更希望我国政务云平台和商业云平台能像国际云厂商一样，以超前眼光快速支持尚在草案阶段的国密混合 PQC 算法，引领我国互联网能快速具备抗量子能力和同时满足用户国密合规需求，为应对未来量子威胁提供一条兼顾合规与安全的可行路径。

三、值得我国专业会议组织者学习的地方

本届 IETF 大会的组织细节也给笔者留下深刻印象，有三点尤其值得借鉴：

- **灵活的"Side Meeting"机制**：当我们申请 TLS 工作组主会议议程未果后，通过申请"Side Meeting"小型研讨会，仍获得了在小范围深入研讨与交流的机会。会议组织方为所有注册参会者提供了清晰的指引和先到先得的会议室预约系统，让无法进入主议程的小众、前沿话题也能有机会得到充分交流，有效保护了创新的萌芽。
- **创新的"HotRFC"环节**：这个环节让任何与会者都有机会用几分钟时间，向全场推介自己天马行空的新想法。这是一个绝佳的"火花碰撞"平台，让创新的想法能迅速找到同路人，非常值得国内技术会议借鉴。
- **高效智能的会议管理**：所有大小会议室均采用无人值守模式，仅预装好配有麦克风、音响、投影和视频会议系统的专用电脑。只需设置主持人电脑为主持人即可用自己的电脑投屏开会，会议室电脑为联席主持人，轻松同步管理线上线下会议。这极大节省了人力成本，保障了会议流程的高效顺畅。

总的来说，首次 IETF 之旅，不仅推动了商密混合 PQC 算法 RFC 草案的社区交流，更深刻感受到了一个开放、包容、高效、由使命驱动的国际标准组织的运作精髓。这些关于“如何让标准真正快速应用起来”的感悟，以及“如何组织一场高效技术会议”的经验，无论是对我们后续的标准推动工作，还是对我国整个互联网行业和密码行业的创新协作，都具有宝贵的参考价值。这趟旅程，收获远超预期。

王高华

2026 年 3 月 23 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 267 篇(共 78 万 5 千多字)和英文 118 篇(16 万 3 千多单词)。