发展我国下一代国密 SSL 证书：国密 MTC 证书

2026 年 5 月 6 日

笔者在 4 月 7 日发表了博文《默克尔树证书(MTC)：下一代 SSL 证书，重塑互联网安全》后，掀起了一股研究 MTC 证书的热潮，有不少朋友私聊问：我国的国密 SSL 证书怎么办？是否也要跟随国际 MTC 证书？笔者的答案是：**必须的**，而且必须抓紧研究。

谷歌和 Cloudflare 主导的 MTC 第一阶段实验始于 2025 年 10 月，目前仍在进行中。实验已实际应用于 1000 多个真实网站，覆盖 Chrome Beta 版约 50%的用户流量。IETF 125 深圳会议公布的数据显示，地标模式 MTC 使 TLS 握手延迟中位数降低约 9%，第 90 百分位降低约 8%。实验团队的结论掷地有声：**“MTC 有效，并且已在保护真实的互联网流量。”**

那么，我国应该怎么办？答案很明确：**发展国密 MTC 证书。**全面借鉴国际 MTC 方案的前瞻性设计，充分融入我国商用密码算法体系、国密证书透明生态和国密证书自动化生态，打造自主可控的下一代国密 SSL 证书体系。以下内容是零信技术的规划与展望，将根据国际标准进展情况同步调整。

一、国际 MTC 方案为何代表下一代方向

传统的 SSL 证书体系是“单件生产”：CA 为每张证书独立签名，客户端独立验证。随着后量子密码（PQC）签名尺寸暴涨（ML-DSA-44 签名 2.4KB、公钥 1.3KB），以及证书有效期缩短至 47 天，签发频率倍增，传统模式难以为继。

MTC 方案的革命性在于“批量生产”：CA 将所有证书构建为一棵 Merkle 树，定期对树根做一次签名，一个树根认证整批证书。更精妙的是**地标模式**：客户端预置地标哈希，服务器仅需发送证书主体和“包含证明”（几百字节），**无需任何签名**，验证极快。**独立模式**作为无地标时的回退，证书中携带签名。其技术特性与传统 SSL 方案对比如下表所示。

技术特性	传统 SSL 方案	MTC 方案	效果
签名方式	每张证书逐个签名	每一批证书一个根签名	大幅减少签名数量
验证方式	直接验证签名	包含证明+地标验证	验证轻量化
证书尺寸	~2-4KB	~1-2KB（含 PQC 公钥）	尺寸显著缩小
日志存储	永久存储	可定期修剪	存储成本可控

谷歌提出的三阶段路线图为：Phase 1（进行中，1000 个网站实测），Phase 2（2027 Q1 邀请 CT 日志运营者），Phase 3（2027 Q3 启动 Chrome 量子抗性根证书库 CQRS）。MTC 的基础是**证书自动化**，实验证书有效期仅 7 天。

二、国密 MTC 证书的技术路线

国密 MTC 证书不是简单地将国际 MTC 中的哈希和签名替换为国产密码算法，而需要从整体架构、模式设计、签名算法演进和过渡策略四个维度进行系统规划。

2.1 总体架构：完全自主的技术组件

- **哈希函数**：全部使用国密 SM3 算法，替代 SHA-256。
- **签名算法**：当前阶段使用国密 SM2 算法，未来平滑过渡至国产 PQC 算法。
- **根证书体系**：基于我国的国家根证书+各 CA 独立根证书的国密根证书认证库。
- **日志服务**：基于国密证书透明日志系统，采用 SM3_SM2 签发 SCT。

2.2 双模式支持：高效与兼容并存

与 MTC 保持一致，国密 MTC 同样支持两种模式：

- **国密地标模式**：证书中不含任何数字签名，仅携带一条从证书叶子到国密地标根的哈希“包含证明”。验证方（国密浏览器）只需预置可信的国密地标哈希，即可完成高效验证。此模式下国密 SSL 证书尺寸可控制在 1.5-2KB（含 SM2 公钥），较传统国密 SSL 证书显著缩小。
- **国密独立模式**：作为平滑升级的兼容机制，证书中携带 SM2 签名，确保在没有地标信息的旧版浏览器上，国密加密连接依然能够正常验证。

2.3 签名算法的分层演进：立足 SM2，迈向 PQC

独立模式证书中携带的签名算法，需要根据产业成熟度分阶段推进：

- **当前阶段（2026-2027）**：采用已广泛部署的 SM2 算法，实现国密 SSL 证书的自动化部署，支持，支持采用国密混合 PQC 算法 SM2MLKEM7658（IANA 编号 4590）实现密钥封装。这是实现国密 MTC 生态落地的基础，也是最稳妥的起点。
- **过渡阶段（2027-2028）**：跟踪国际 PQC 标准（如 ML-DSA-44），参考 IETF 草案和国际 CA 的多 cosigner 签名方案，在独立模式证书中逐步引入国际 PQC 签名作为可选能

力。

- **未来阶段（2028 年后）**：聚焦国产 PQC 算法，在适当阶段实现国产 PQC 签名在国密 MTC 独立模式中的替换，实现从“自主可控”到“量子安全”的平滑演进。

2.4 与传统国密证书的平滑过渡

国密 MTC 生态的推广必须做到新旧兼容。建议分三个阶段完成过渡，这种渐进式策略已成功运用于 TLS 1.3 国密和国密 CT 的部署，确保现有国密 SSL 证书实现 HTTPS 加密的业务不中断。

实施阶段	国密 SSL 证书模式	国密 MTC 独立模式	国密 MTC 地标模式
第一周期（传统）	✅ 仅支持	❌	❌
第二周期（试点）	✅ 主力支持	✅ 支持	❌
第三周期（全面）	备选降级	✅ 主力支持	✅ 优先支持

2.5 国密 MTC 证书的技术优势

与传统国密 SSL 证书相比，国密 MTC 证书将带来了多项核心优势：

- **尺寸更小，体验更快**：国密 MTC 证书一旦切换到地标模式，证书尺寸将缩小到极致，大幅提升国密 HTTPS 加密的连接体验。
- **带宽更低，连接更稳**：移动互联网环境下，国密 MTC 证书的快速签发与紧凑传输，将直接降低数据包传输时间和延迟。
- **验证可审计，运营更安全**：通过国密 CT 日志存档和地标可审查机制，让 CA 机构与最终用户能随时验证任何国密 MTC 证书的生命周期。
- **面向未来，随时适配 PQC**：一旦我国未来确定国产后量子密码签名算法标准，只需替换国密地标模式中的“包含证明”和算法兼容，即可无缝升级。

三、零信技术的端云一体解决方案

技术路线清晰之后，关键是有没有能力落地。零信技术经过近 5 年的持续投入，已经构建起从 CA 系统、日志系统、浏览器到网关的全链条能力，为形成了端云一体的国密 MTC 生态打下了坚实基础。

3.1 四把钥匙：已经具备的核心能力

第一把钥匙：零信国密证书透明日志系统。2022 年全球独家发布，目前已有连续 5 年更

新密钥的 3 个国密 CT 日志系统，全部采用 SM3/SM2 国密算法，零信浏览器信任验证，为多家 CA 提供近 5 年稳定国密 CT 服务，签发的国密 SSL 证书超过 10 万张。这正是 MTC 地标模式所需的核心根基。

第二把钥匙：零信浏览器。基于 Chromium 内核，全面支持国密 SSL、SM2 算法、国密 CT 验证、国密混合 PQC 算法。将扩展其验证引擎，使其同时支持国际 MTC 证书和国密 MTC 证书。

第三把钥匙：零信云 SSL 服务系统。已完成连续多月的每日自动化签发实验，验证了双证书（RSA+SM2）自动化签发能力。这是高频 MTC 签发的基础，也为 7 天有效期证书的规模化签发做好了技术储备。

第四把钥匙：零信 HTTPS 加密自动化网关。服务端 MTC 证书的关键支撑，可自动化完成国密 MTC 证书的申请、验证、部署和更新，并根据客户端能力自适应切换加密模式，为不支持国密的浏览器提供国际 SSL 证书和国际 MTC 证书，为最新版零信浏览器提供国密 MTC 地标模式，真正实现端云一体闭环。

3.2 五步行动计划：从规划到落地

零信技术将紧跟国际标准动态，当前规划如下：

第一步：紧跟标准。已加入负责制定 MTC 证书 RFC 国际标准的 IETF PLANTS 工作组，跟踪 MTC RFC 进展和谷歌 CQRS 细则，确保国际 MTC 证书签发能力与 Chrome 根证书库要求对齐，同时优先让国密 MTC 方案保持同步演进。

第二步：升级国密 CT 系统。增加新日志条目类型（如 tbs_cert_entry），支持记录国密 MTC 证书的原始信息，签发 SM2_SM3 的 SCT；支持日志修剪和地标分发接口。

第三步：升级云 SSL 服务系统。 支持签发国密 MTC 证书（地标模式和独立模式），继续支持双证书透明（国际 CT+国密 CT）。

第四步：完善自动化网关。 零信 HTTPS 加密自动化网关将率先实现国密 MTC 证书的自动化申请、部署和更新，根据浏览器能力自适应选择最优加密模式，实现用户无感升级。

第五步：推动标准制定。 计划向密码标委会提交国密 MTC 技术方案和应用实践报告，牵头或参与制定国密 MTC 证书标准，与产业伙伴共同推动国密 MTC 证书成为我国网络信任体系的核心基础设施。

四、抢占技术先机，积极拥抱国密 MTC 证书

如同国际 PKI 领域出现的 MTC 方案一样，我国国密 SSL 证书正站在技术跃升的关键临界

点上。零信技术基于在国密证书透明领域近 5 年的技术积淀，以及已完成连续多月的每日证书自动化签发证书实验所积累的实践经验，已经构建起从 CA 签发系统、证书透明日志、浏览器验证，到自动化网关部署的**端云一体全生态能力**。

我们不只是在等待，我们一直在行动。面对 MTC 证书这个国际下一代 SSL 证书即将带来的生态重构契机，零信技术已做好充分准备，将全力打造国密 MTC 证书全生态产品。

在此，我们诚挚邀请所有专注于国密算法创新、国密证书服务和国产密码技术应用普及的专业人士、CA 机构与广大用户，与我们携手合作。当全球互联网安全技术浪潮来临之际，唯有主动拥抱变革、锐意创新，共同守护数字时代国家网络空间的安全与稳定。

王高华

2026 年 5 月 6 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 273 篇(共 81 万 1 千多字)和英文 119 篇(16 万 6 千多单词)。