# 默克尔树证书(MTC)：下一代 SSL 证书，重塑互联网安全

2026 年 4 月 7 日

## 一、SSL 证书为何不行了？

每天，当你访问一个网站时，浏览器与服务器之间都会进行一次复杂的“握手”仪式。这个仪式中，服务器会出示一张数字身份证——SSL/TLS 证书，证明自己就是你要访问的那个网站，而不是某个冒名顶替者。这张证书背后，支撑着整个互联网信任体系的基石：公钥基础设施（PKI）。

这套体系成功运行了 32 年，但它正在逼近极限。**第一个压力来自即将到来的量子计算时代**。美国已经推出了后量子密码数字签名算法标准，如 ML-DSA。但这些新算法的尺寸令人震惊：一个 ML-DSA-44 的签名就高达 2420 字节，公钥也有 1312 字节，而当前广泛使用的 ECDSA P-256 签名只有 64 字节。这意味着，如果直接替换，一个典型 TLS 握手携带的签名和公钥总量将从几百字节暴涨到数十千字节。

**第二个压力来自证书透明（CT）**。为了检测 CA 是否滥发证书，浏览器要求每张证书必须被提交到至少两个公共证书透明日志中，并附带日志签名（SCT）在证书中。目前的标准要求每张证书至少附带两个 SCT，每个 SCT 又是一次签名。这相当于在原有基础上又增加了两层签名。

这两个因素叠加，使得未来一张后量子证书的“包装”尺寸可能达到 **10KB** 甚至更高。对于每个 TLS 连接来说，这不仅是网络负担，更是计算负担——签名验签是 CPU 密集型操作，移动设备、物联网终端将面临显著的性能下降和功耗增加。

更加棘手的是，**证书生命周期正在缩短**。为了应对证书滥发和密钥泄露风险，以及实现敏捷的后量子密码迁移，行业趋势已将证书有效期从 398 天缩短到 47 天，将来甚至更短。这意味着 CA 的签发频率将提高两个数量级，证书透明日志系统的存储和计算压力呈指数级增长。传统 PKI 架构中，每张证书都需要独立处理、独立签名、独立入日志库，这种“单件生产”模式在高频签发场景下难以为继。

## 二、默克尔树证书是怎么解决难题的？

面对这三重压力，谷歌、Cloudflare 等公司联合向 IETF 提交了一份名为“默克尔树证书”（Merkle Tree Certificates，简称 MTC）的新方案。其核心思路可以概括为四个字：**化零为整**。

### 1. 批量认证取代逐个签名

在传统模式下，CA 每签发一张证书，就要对它进行一次数字签名。MTC 的做法是“先入日志，再生成证书”。每个 CA 必须维护一个自己的日志系统，每签发一张证书，不是直接签名证书本身，而是将证书的核心信息（TBSCertificateLogEntry）作为一条记录追加到日志中。这个日志用 Merkle 树结构组织——每个叶子节点是一条证书记录，父节点是子节点哈希值的哈希。

关键的一步来了：CA 不对单张证书签名，而是定期对**树根（Checkpoint）**进行签名。一个树根签名，就相当于同时认证了该时刻日志中所有证书的真实性。如果一张证书被篡改，其哈希值会改变，最终导致树根哈希值不匹配，签名验证失败。

### 2. 包含证明取代多重签名

客户端如何验证一张具体证书呢？MTC 证书本身携带的不是传统签名，而是一个**包含证明（Inclusion Proof）**——从证书所在叶子节点一路向上到树根的哈希路径。客户端只需要获得可信的树根，就能用这个证明验证证书是否真实存在于 CA 的日志中。

这里还有一个巧妙的设计：MTC 证书支持两种工作模式：

**(1) 地标模式（Landmark Mode）**：系统定期选出一些树根作为“地标”，将这些地标的哈希值预先分发到浏览器等客户端。当服务器需要出示证书时，如果客户端已有对应地标，服务器只需发送证书主体和**包含证明**，**无需任何签名**。一个包含证明仅几百字节，远小于后量子密码算法签名。

**(2) 独立模式（Standalone Mode）**：如果客户端没有对应地标（如首次访问或长时间未更新），服务器可发送携带 1~3 个第三方见证者（Cosigner）签名的证书作为回退路径。虽然尺寸稍大（约 3~8KB），但保证兼容性。

两种模式共存，客户端与服务器通过 TLS 1.3 扩展自动协商选择最优模式，在性能和兼容性之间取得平衡。

### 3. 日志可裁剪降低存储压力

MTC 的另一个创新是日志可以“修剪”。传统 CT 日志必须永久保留所有证书，而 MTC 允许 CA 在证书过期后，将日志的早期部分裁剪掉，只保留哈希值作为“存根”。这大大降低了长期存储成本，使得维持高频签发成为可能。这就好比：传统 SSL/TLS 证书像是每笔交易回单都要找银行盖章，而 MTC 像是银行每月出一份对账单，客户只需要拿到对账单就能证明所有交易的真实性。

## 三、未来展望：从量子安全到 CA 角色重塑

未来已来，新一代互联网安全基座已经浮出水面，全球业界正在为赢得这个世纪商机而悄悄忙碌中，浏览器厂商、CA 机构、互联网厂商都有巨大的市场机会，就看谁能看懂了。

### 1. MTC 证书落地计划

MTC 目前仍处于 IETF 草案阶段，但一项由 Cloudflare 与谷歌 Chrome 团队主导的**三阶段部署计划**已经在 2025 年 10 月正式启动。

**(1) 阶段 1（进行中）**：真实环境可行性测试。

Cloudflare 与 Chrome 合作，在真实互联网流量中测试 MTC。目前已有 **1000 个真实网站**启用了 MTC，覆盖 Chrome Beta 版约 50%的用户流量。每张 MTC 证书都同时由一张传统受信任的 SSL 证书作为“安全备胎”，确保即使 MTC 验证路径出现问题，连接仍然可信。

这个阶段的初步实验成果已于 2026 年 3 月 16 日在 **IETF 125** 深圳大会上公布，得出了三个关键结论：

- **性能提升显著**：即使与传统 ECC 算法 SSL 证书相比，地标模式 MTC 仍使 TLS 握手延迟中位数降低约 **9%**（105ms vs 116ms），第 90 百分位降低约 **8%**（348ms vs 380ms）。预期在后量子密码时代，性能优势将更为悬殊。
- **客户端更新迅速**：大多数 Chrome Beta 用户的地标在 **2-3 小时内完成更新**，稳态下仅有 **0.5%-1.5%** 的客户端使用过时地标（需回退到独立模式）。
- **部署障碍可控**：实验中未发现中继设备（middlebox）对 MTC 证书造成明显干扰，验证了 TLS 1.3 对证书加密的保护作用。

实验团队在 PPT 中给出的结论是：**“MTC 有效，并且已在保护真实的互联网流量。”**

**(2) 阶段 2（2027 年第一季度）：**证书透明日志运营者加入

谷歌将邀请合格的证书透明日志运营者加入，帮助引导公共 MTC 签发。这意味着 MTC 将从 Cloudflare 的单点实验走向多方参与的生态建设，证书透明日志运营者将成为 MTC 信任网络中的重要节点。

**(3) 阶段 3（2027 年第三季度）：**启动量子安全根认证计划

谷歌将正式启动**谷歌浏览器量子安全根认证计划-CQRS**（Chrome Quantum-resistant Root Store），发布最终的 CA 接入规则，并建立仅支持 MTC 的全新量子安全根证书库。这一阶段标志着 MTC 从实验走向规模化部署。

谷歌 CQRS 计划已经明确了几个关键原则：

- **MTC 是一种全新的紧凑型抗量子证书格式**，专为公共 HTTPS 加密设计。它不是对现有证书格式的修补，而是一次彻底的重新设计。
- **谷歌将发布一个全新的、仅支持 MTC 的根证书库**，而不是试图将后量子密码算法“塞进”现有的传统密码算法根证书库中。Chrome 明确表示“暂无计划将包含后量子算法的传统 SSL 证书添加到现有根证书库”。
- **MTC 面向所有公共 CA 开放**，但 CA 的接入将是渐进的，取决于各 CA 是否完成 MTC 签发系统的开发与部署。届时将建立配套的根证书计划，明确 CA 的准入规则和运营要求。

## 2. MTC 生态的可能形态：从协议到落地【作者预测】

IETF 草案为 MTC 定义了精妙的技术协议，但一个完整的生态系统远不止于此。浏览器如何获取上百个 CA 每小时产生的地标？CA 如何被纳入信任体系？这些问题草案刻意留白，等待生态自然演化。笔者基于对证书透明生态的观察，大胆预测未来 MTC 生态的几个关键特征：

**(1) 地标聚合器：中间层的必然崛起**

CT 生态的成功经验表明，让每个浏览器直接对接所有 CA 的日志系统是不可行的。CT 采用“日志聚合监控服务”作为中间层，MTC 生态中，很可能出现类似的**地标聚合器**——第三方服务定期从所有参与 CA 拉取地标，验证 CA 签名后打包成聚合列表，再用自己的私钥签名发布。浏览器只需内置少量地标聚合器公钥，定期下载聚合列表（每日不足 1MB），即可获得全网地标视图。

**(2) 多聚合器冗余与公开审计**

为防止单一聚合器作恶，生态将支持多个独立聚合器并存。它们之间相互验证数据一致性，任何篡改行为都会被公开审计发现并迅速剔除。这与 CT 要求 SSL 证书出现在多个日志中的设计哲学一脉相承。

**(3) 渐进过渡：三证并存的数年窗口**

未来数年内，服务器将同时提供三种证书：传统 SSL 证书（兼容旧客户端）、MTC 地标模式证书（最优性能）、MTC 独立模式证书（回退路径）。通过 TLS 1.3 扩展协商，客户端与服务器将自动选择双方支持的最优模式。这种渐进式部署策略，与 TLS 1.3、CT 的落地路径高度相似，是互联网基础设施升级的成功经验。

上述预测能否成真，取决于 2027 年谷歌 CQRS 细则的最终公布，以及 CA、浏览器、聚合器运营者之间的博弈与协作。但可以确定的是，MTC 绝非简单的性能优化，它正在重塑互联网信任体系的底层架构。

## 3. CA 的机会：从“签名工坊”到“可信日志运营者”

MTC+CQRS 的组合将深刻改变 CA 的角色。传统 CA 的核心能力是“保管根签名私钥”、“执行域名验证”和“签发证书”。而在新体系下的变化有：

**第一：日志运营成为核心能力**。MTC 要求每个 CA 维护自己的公开证书透明日志，日志的可用性、完整性和裁剪策略将直接影响证书的信任度。能够高效运营大规模 Merkle 树日志的 CA 将获得竞争优势。

**第二：见证者可能催生新业务**。MTC 依赖第三方“见证者”（Cosigner）来为子树签名，这些见证者可以是独立机构、浏览器厂商或 CA 自身。提供高可用、地理分布、合规审计的见证服务，可能成为一个独立的细分市场。

**第三：域名验证服务与日志深度绑定**。由于 MTC 的证书必须通过日志来证明有效性，CA 需要将域名验证过程与日志追加操作原子化处理。这意味着 CA 的自动化签发系统（如 ACME）需要重新设计，以支持“验证即入库”的模式。

**第四：小型 CA 面临整合压力**。运营 Merkle 树日志、维护见证关系、应对高频签发，对技术架构和资金投入提出了更高要求。这可能会加速行业整合，促使小型 CA 转向“CA 即服务”平台，将底层基础设施外包给专业服务商，或者被迫退出 CA 市场。

**第五：量子迁移成为差异化机会**。随着量子计算威胁日益临近，能够提供平滑、高效、向

后兼容的抗量子证书迁移方案的 CA，将在企业客户中获得明显优势。MTC+CQRS 的组合恰好为此提供了一个可落地的技术路径。

**第六：CA 准入迎来新门槛**。谷歌 CQRS 计划将明确：只有通过根证书计划审核、并满足 MTC 技术要求的 CA，才能被纳入地标分发体系。这些要求包括：公开 Merkle 树日志访问地址、定期生成并签名地标、允许聚合器拉取数据、接受公众审计。全球 CA 若想继续在新的 Web PKI 中占有一席之地，必须在规定时限内完成 MTC 系统改造——这既是挑战，也是洗牌的机会。而对于国内 CA 而言，由于起步晚，已经完全失去了传统密码算法 CA 体系的市场机会，是否能抓住这个后量子密码全新体系的机会，就要看各家 CA 是否能领悟到这个未来 50 年的世纪商机了。

## 四、默克尔树证书将重塑互联网安全底座

默克尔树证书不是对传统 PKI 体系的修修补补，而是一次从“单件生产”到“批量制造”的范式转换。它将证书透明从外部约束内化为系统核心，用 Merkle 树的数学结构替代了多重签名的堆叠，为后量子密码时代预留了性能空间。

随着 2025 年底真实环境测试的推进和 3 月份的初步实验结果的公布，以及 2027 年谷歌 CQRS 的正式启动，MTC 正在从互联网标准草案走向生产实践。对于 CA 行业而言，这是一次挑战，更是一次重塑自身价值、拓展服务边界的历史机遇。未来两年，我们将看到第一批公共 CA 正式接入 MTC 体系，互联网安全的底层架构，正在静悄悄地进行一次代际跃迁。祝愿中国 CA 们能及时抓住这个世纪机遇！

王高华

2026 年 4 月 7 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 269 篇(共 79 万 4 千多字)和英文 119 篇(16 万 6 千多单词)。