Merkle Tree Certificates: Reshaping Internet Security

April 7, 2026

1. Why SSL/TLS Certificates Are No Longer Sufficient

Every day, when you visit a website, browser and the server perform a complex "handshake" ritual. During this ritual, the server presents a digital ID card—an SSL/TLS certificate—proving it is the website you intend to visit, not an impostor. Behind this certificate lies the cornerstone of the Internet's trust infrastructure: the Public Key Infrastructure (PKI).

This system has been operating for 32 years, but it is approaching its limits. **The first pressure comes from the impending quantum computing era.** The NIST has already released standards for post-quantum cryptography algorithms, such as ML-DSA. However, the size of these new algorithms is staggering: an ML-DSA-44 signature is 2,420 bytes, and its public key is 1,312 bytes, compared to just 64 bytes for the widely used ECDSA P-256 signature. This means that if directly replaced, the total size of signatures and public keys carried in a typical TLS handshake would explode from a few hundred bytes to tens of kilobytes.

The second pressure comes from Certificate Transparency (CT). To detect whether CAs are issuing certificates improperly, browsers require that every certificate be submitted to at least two public logs and include signed certificate timestamps (SCTs). Current standards require two SCTs per certificate at least, each signature adding another layer. This effectively adds two more signatures on top of the existing ones.

Combined, these factors mean that a future post-quantum certificate's "packaging" could exceed 10K bytes. For each TLS connection, this is not only a network burden but also a computational one—signature verification is CPU-intensive, and mobile devices and IoT endpoints will face significant performance degradation and increased power consumption.

Even more challenging is the **shortening of certificate lifetimes**. To mitigate risks from improper issuance, key compromise and PQC migration, industry trends are pushing certificate validity periods down from 398 days to 47 days, even shorter in the future. This means CA issuance frequency will increase by two orders of magnitude, putting exponential pressure on CT log system storage and computation. In the traditional PKI architecture, each certificate is processed, signed, and CT logged independently—this 'single-item production' model is difficult to sustain in high-frequency issuance scenarios.

2. How Merkle Tree Certificates Solve These Problems

Faced with these three pressures, Google, Cloudflare, and others have jointly submitted a new solution to the IETF called "Merkle Tree Certificates" (MTC). Its core idea can be summarized in a word: consolidate many into one.

(1) Batch Authentication Replaces Per-Certificate Signatures

In the traditional model, a CA signs each certificate individually. MTC flips this process: "log first, certificate later." The CA maintains its own log. For each certificate issued, instead of signing the certificate itself, the CA appends the certificate's core information (TBSCertificateLogEntry) as a record to the log. This log is organized as a Merkle tree—each leaf node is a certificate record, and each parent node is the hash of its children.

The crucial step: the CA does not sign individual certificates but instead periodically signs the **tree root (Checkpoint)**. One root signature simultaneously authenticates every certificate in the log at that moment. If a single certificate is tampered with, its hash changed, ultimately causing the root hash to mismatch and the signature verification to fail.

(2) Inclusion Proofs Replace Multiple Signatures

So how does a client - browser verify a specific certificate? An MTC certificate itself does not carry a traditional signature but rather an **Inclusion Proof**—the hash path from the leaf node representing the certificate up to the root. If the client has a trusted root hash, it can use this proof to verify that the

certificate truly exists in the CA's log.

MTC certificates support **two operational modes**:

- **Landmark Mode:** The system periodically selects certain tree roots as "landmarks" and pre-distributes their hash values to clients like browsers. When a server needs to present a certificate, if the client already has the corresponding landmark, the server only needs to send the certificate body and the **inclusion proof**—**no signature is required**. The inclusion proof is only a few hundred bytes, far smaller than a post-quantum algorithm signature.

- **Standalone Mode:** If the client lacks the corresponding landmark (e.g., first-time visit or long period without updates), the server can send a certificate carrying 1-3 signatures from third-party cosigners as a fallback path. While larger (approximately 3-8 KB), this ensures compatibility.

The two modes coexist, with client and server automatically negotiating the optimal mode via TLS 1.3 extensions, striking a balance between performance and compatibility.

(3) Log Pruning Reduces Storage Pressure

Another innovation of MTC is log pruning. Traditional CT logs must permanently retain all certificates, while MTC allows a CA to prune older portions of the log after certificates expire, retaining only hash values as "stubs." This significantly reduces long-term storage costs, enabling high-frequency issuance. This is just like: traditional SSL/TLS certificates are like getting each transaction notarized individually, while MTC is like receiving a monthly bank statement that proves all transactions at once.

3. Outlook: From Quantum Security to the Evolution of CA Roles

The future is here, and the new generation of Internet security infrastructure has already emerged. The global industry is quietly preparing to seize this once-in-a-century business opportunity. Browsers, CAs, and Internet companies all have huge market opportunities; it depends on who can understand it.

(1) MTC Implementation Plan

The MTC specification is still in the IETF draft stage, but a **three-phase deployment plan** led by Cloudflare and Google Chrome was officially launched in October 2025.

Phase 1 (Ongoing): Real-world feasibility testing.

Cloudflare and Chrome are collaborating to test MTC on live Internet traffic. Currently, **1,000 real websites** have MTC enabled, covering approximately 50% of Chrome Beta user traffic. Each MTC certificate is backed by a traditional, trusted SSL/TLS certificate as a "safety spare tire" ensuring connections remain trusted even if the MTC verification path encounters issues.

The preliminary experimental results of this stage were announced at the IETF 125 Shenzhen meeting on March 16, 2026, and three key conclusions were drawn:

- **Significant Performance Gains:** Even when compared to traditional ECDSA SSL/TLS certificates (non-post-quantum), Landmark Mode MTC reduced median TLS handshake latency by approximately **9%** (105ms vs 116ms) and 90th percentile latency by approximately **8%** (348ms vs 380ms). The performance advantage is expected to be even more dramatic in the post-quantum era.
- **Rapid Client Updates:** Most Chrome Beta clients updated their landmarks within **2-3 hours**, with only **0.5%-1.5%** of clients in steady state using outdated landmarks (thus falling back to Standalone Mode).
- **Manageable Deployment Obstacles:** The experiment found no significant interference from middleboxes on MTC certificates, validating TLS 1.3's encryption protection for server certificates.

The experiment team concluded in their presentation: **"MTCs work (!), and are used to secure real Internet traffic today."**

Phase 2 (Q1 2027): Invite Qualified Certificate Transparency Log Operators.

Google will invite qualified Certificate Transparency log operators to join and help guide public MTC issuance. This means that MTC will move from Cloudflare's single-point experiment to a multi-party participatory ecosystem, and Certificate Transparency log operators will become important nodes in the MTC trust network.

Phase 3 (Q3 2027): Official launch of Chrome Quantum-resistant Root Store.

Google will officially launch **CQRS (Chrome Quantum-resistant Root Store)**, publication of final CA onboarding rules, and establishment of a new root store exclusively supporting MTC. This stage marks the transition of MTC from experimentation to large-scale deployment.

The Google CQRS program has clarified several key principles:

- **MTC is a completely new, compact, quantum-resistant certificate format** designed for public HTTPS. It is not a patch to existing certificate formats but a ground-up redesign.
- **Google will release a brand-new root store that only supports MTC**, rather than attempting to "shoehorn" post-quantum algorithms into the existing traditional root store. Chrome has explicitly stated it has "no current plan to add traditional SSL/TLS certificates with post-quantum algorithms to the existing root store."
- **MTC is open to all public CAs**, but adoption will be gradual, depending on each CA's implementation of MTC issuance systems. A supporting root store program will be established to define CA admission rules and operational requirements.

(2) The Likely Shape of the MTC Ecosystem: From Protocol to Deployment [Author's Prediction]

The IETF draft defines an elegant technical protocol, but a complete ecosystem involves much more. How will browsers obtain hourly landmarks from hundreds of CAs? How will CAs be incorporated into the trust system? The draft intentionally leaves these questions open for the ecosystem to evolve naturally. Drawing on observations from the Certificate Transparency ecosystem, we can make some educated predictions about key features of the future MTC ecosystem:

- **Landmark Aggregators: The Inevitable Rise of an Intermediary Layer**

  The success of the CT ecosystem shows that having every browser directly interface with every log is impractical. CT uses "log aggregators and monitors" as an intermediary layer. In the MTC ecosystem, similar **Landmark Aggregators** are likely to emerge—third-party services that periodically pull landmarks from all participating CAs, verify the CA signatures, package them into aggregated lists, and sign the results with their own private keys. Browsers would only need to embed a few aggregator public keys and periodically download the aggregated list (less than 1 MB per day) to obtain a complete view of all landmarks.

- **Multi-Aggregator Redundancy and Public Audit**

  To prevent a single aggregator from misbehaving, the ecosystem will likely support multiple, independent aggregators. They would cross-verify data consistency with each other, and any tampering would be detected by public audits and swiftly removed. This aligns with the CT design philosophy of requiring certificates to appear in multiple logs.

- **Gradual Transition: A Multi-Year Window with Three Certificate Types**

  For several years, servers will likely provide three types of certificates simultaneously: traditional SSL/TLS certificates (for legacy clients), MTC Landmark Mode certificates (optimal performance), and MTC Standalone Mode certificates (fallback path). Through TLS extension negotiation, clients and servers will automatically select the best mutually supported mode. This gradual deployment strategy mirrors the successful rollout paths of TLS 1.3 and CT—a proven approach for upgrading fundamental internet infrastructure.

Whether these predictions hold true will depend on the final details of the CQRS rules announced in 2027 and the subsequent collaboration and competition among CAs, browsers, and aggregator operators. What is certain, however, is that MTC is far more than a mere performance optimization; it is fundamentally reshaping the underlying architecture of the internet's trust system.

(3) Opportunities for CAs: From "Signature Workshops" to "Trusted Log Operators"

The combination of MTC and CQRS will profoundly change the role of CAs. The traditional core competencies of CAs—"holding CA signing private keys", "performing domain validation" and “issuing certificate”—will expand significantly in the new system:

First, Log Operation Becomes a Core Competency. MTC requires each CA to maintain its own public log. The log's availability, integrity, and pruning policies will directly impact the trustworthiness of certificates. CAs capable of efficiently operating large-scale Merkle Tree logs will gain a competitive advantage.

Second, Cosigner May Give Rise to New Business Models. MTC relies on third-party cosigners to

sign subtrees. These cosigners could be independent organizations, browsers, or the CAs themselves. Providing high-availability, geographically distributed, auditable cosigning services could become a distinct market segment.

Third, Domain Validation Becomes Tightly Integrated with Logging. Because an MTC certificate's validity is proven through the log, CAs need to atomically combine the domain validation process with log appending. This means CA certificate automation systems (like ACME) need to be redesigned to support a "validate-and-log" model.

Fourth, Smaller CAs Face Consolidation Pressure. Operating a Merkle Tree log, maintaining cosigner relationships, and handling high-frequency issuance requires significant technical infrastructure and investment. This may accelerate industry consolidation, prompting smaller CAs to shift towards "CA-as-a-service" platforms that outsource the underlying infrastructure to specialized providers, or be forced to withdraw from the CA industry.

Fifth, Quantum Migration Becomes a Key Differentiator. As the quantum computing threat looms, CAs that can offer smooth, efficient, and backward-compatible post-quantum certificate migration paths will gain a significant advantage with enterprise customers. The MTC+CQRS combination provides a concrete technical path for this.

Sixth, CA Admission Faces New Hurdles. Google's CQRS plan will specify that only CAs that pass root store program audits and meet MTC technical requirements will be included in the landmark distribution system. These requirements will include: publicly exposing the Merkle Tree log, periodically generating and signing landmarks, allowing aggregators to pull data, and submitting them to public audit. Traditional CAs wishing to maintain a place in the Web PKI must complete their MTC system transformation within the specified timeline—a challenge, but also an opportunity for reshuffling the deck.

4. Merkel Tree Certificates Will Reshape the Foundation of Internet Security

Merkle Tree Certificates are not a minor patch to the traditional PKI system, but a paradigm shifts from

"piecemeal production" to "batch manufacturing." They integrate Certificate Transparency from an external requirement into a core system feature, replacing stacked multiple signatures with the mathematical structure of Merkle trees, and reserve performance headroom for the post-quantum era. With real-world testing advancing since late 2025 and the announcement of the preliminary experimental results in March, then the official launch of CQRS planned for 2027, MTC is moving from an internet draft to a production reality. For the CA industry, this is both a challenge and a historic opportunity to reshape their value proposition and expand their service boundaries. Over the next two years, we will likely see the first public CAs formally onboard the MTC ecosystem. The foundational architecture of Internet security is quietly undergoing a generational shift.

Richard Wang

April 7, 2026
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 119 articles in English (more than 166K words) and 269 articles in Chinese (more than 794K characters in total).