

Why Post-Quantum Changes the Economics of the Internet

Merkle Tree Certificates and the Future of the WebPKI

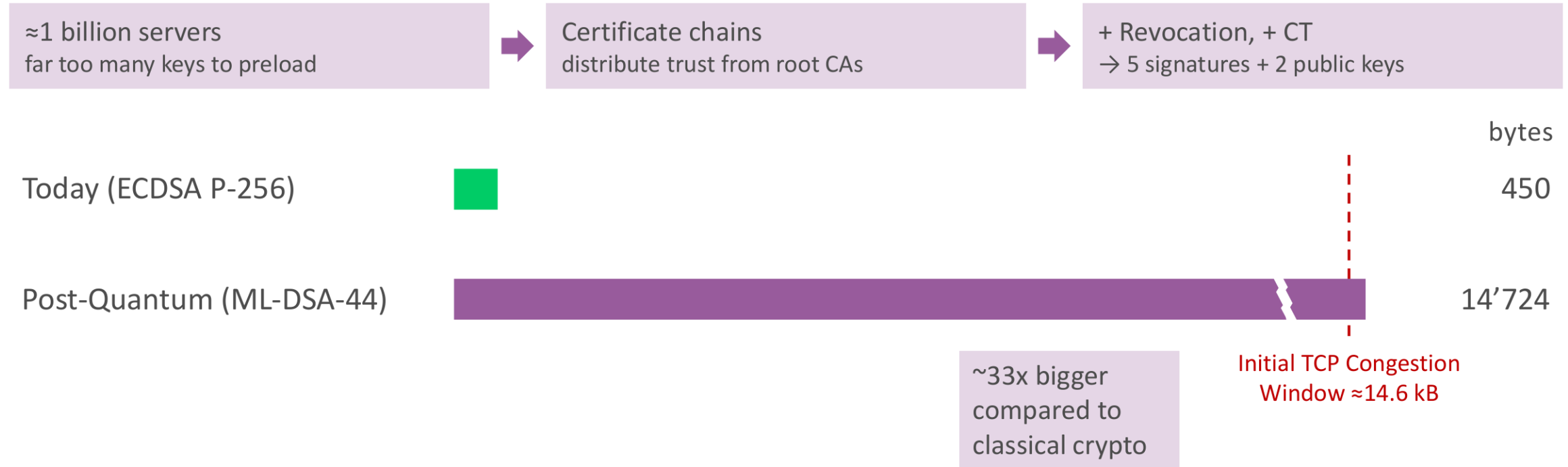
Fabio Banfi and Benjamin Rothenberger | 20.10.2026 | Swiss Cyber Storm 2026

**“Post-quantum signatures
are ready...**

**The Internet just can't afford
them.”**

The Problem

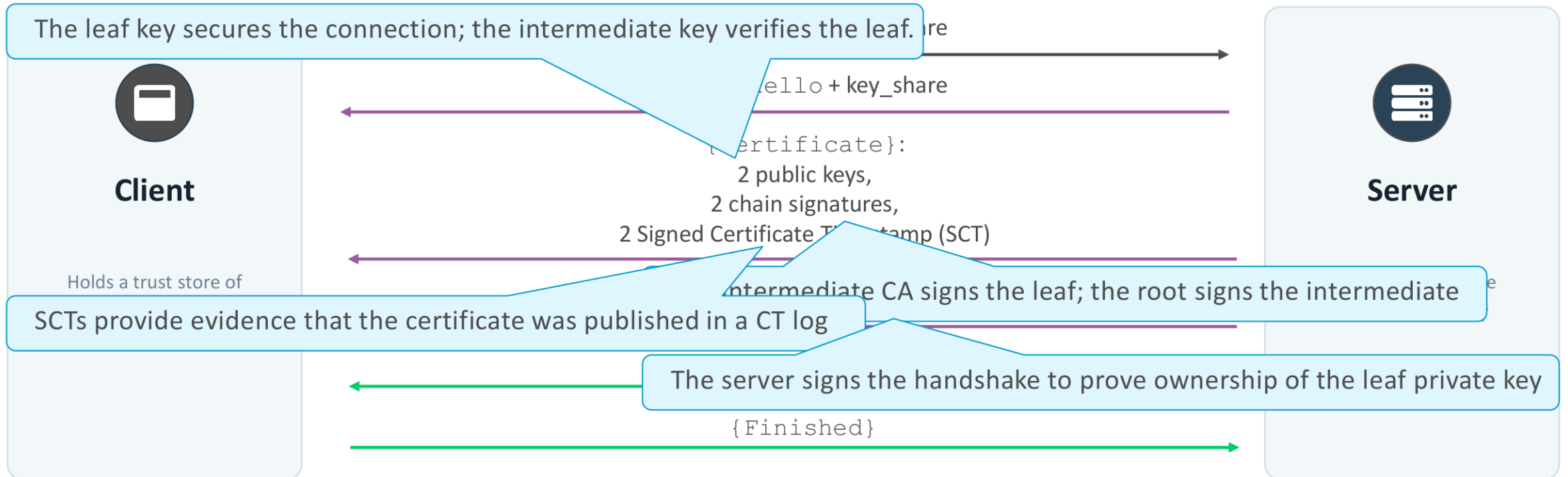
Not a niche problem: every TLS handshake on the Internet pays



The fix is surprising:
We don't make signatures smaller.
We delete them. Four out of five.

The TLS Handshake at a Lower Level

How many cryptographic objects are exchanged for **authentication**?



On the wire:



In total, we transmit 2 public keys and 5 signatures just for authentication

What changes now with the rise of Quantum Computers?

	Scheme	Security level		How many bits need to be brute-forced to break the scheme
		Pre-quantum	Post-quantum	
Symmetric	AES-128	128	64*	} Double the key size!
	AES-256	256	128*	
	SHA2-256	256	128*	
	SHA3-256	256	128*	
Asymmetric	(EC)DH-3072	128	Broken	} Find new schemes!
	(EC)DSA-3072	128	Broken	
	RSA-3072	128	Broken	

Asymmetric cryptography is considered broken!
This affects both *confidentiality* and *authentication* in TLS.

Two Post-Quantum Problems in TLS

Post-quantum key exchange and post-quantum authentication fail in different ways



Confidentiality: **urgent**, but **deployed**

- Harvest now, decrypt later:
adversaries record today, decrypt later
- ✓ ■ Solution available: hybrid X25519MLKEM768
- ✓ ■ Migration is simple and already done:
~67% of human traffic to Cloudflare
- ✓ ■ PQ overhead is ok:
one key share each way, ~1.1–1.2 kB



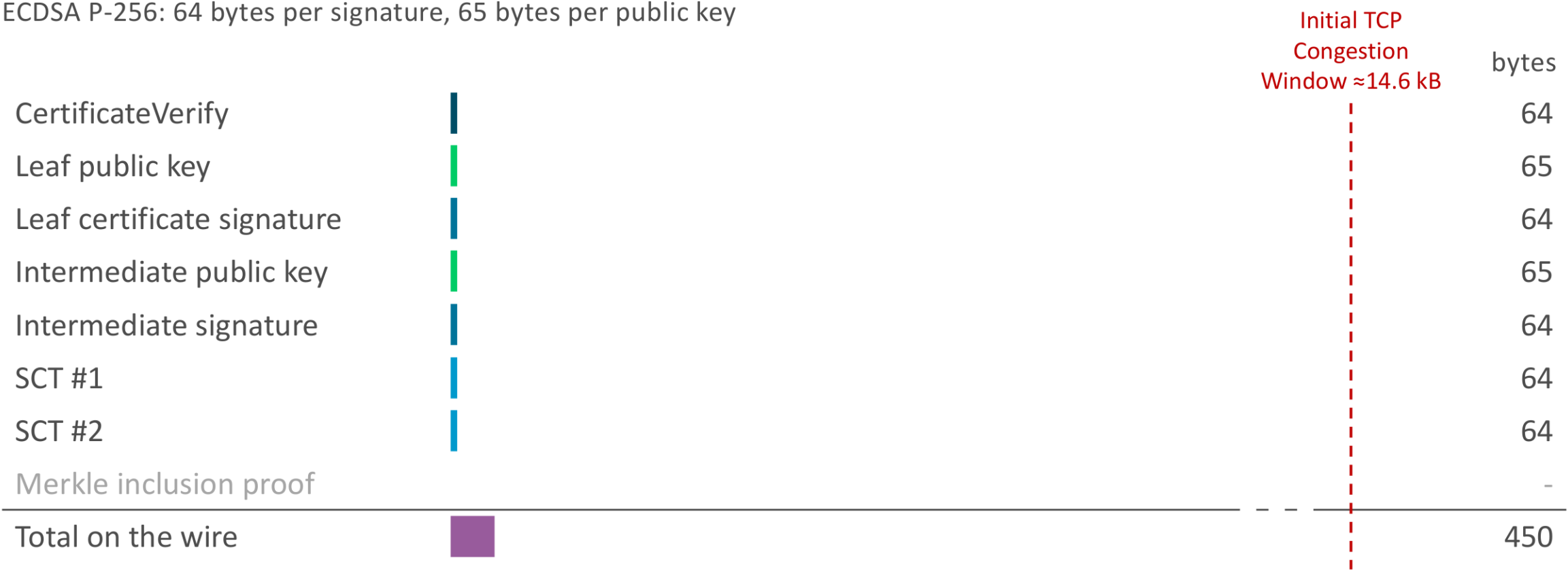
Authentication: **not urgent**, but **harder**

- Forgery needs a live quantum computer:
nothing to harvest today
- ✗ ■ Solution not available yet
- ✗ ■ Migration is ecosystem-wide and complex:
root programs, CAs, logs, every client
- ✗ ■ PQ overhead is a problem:
5 signatures + 2 public keys, ~15 kB

The bottleneck is authentication, not encryption

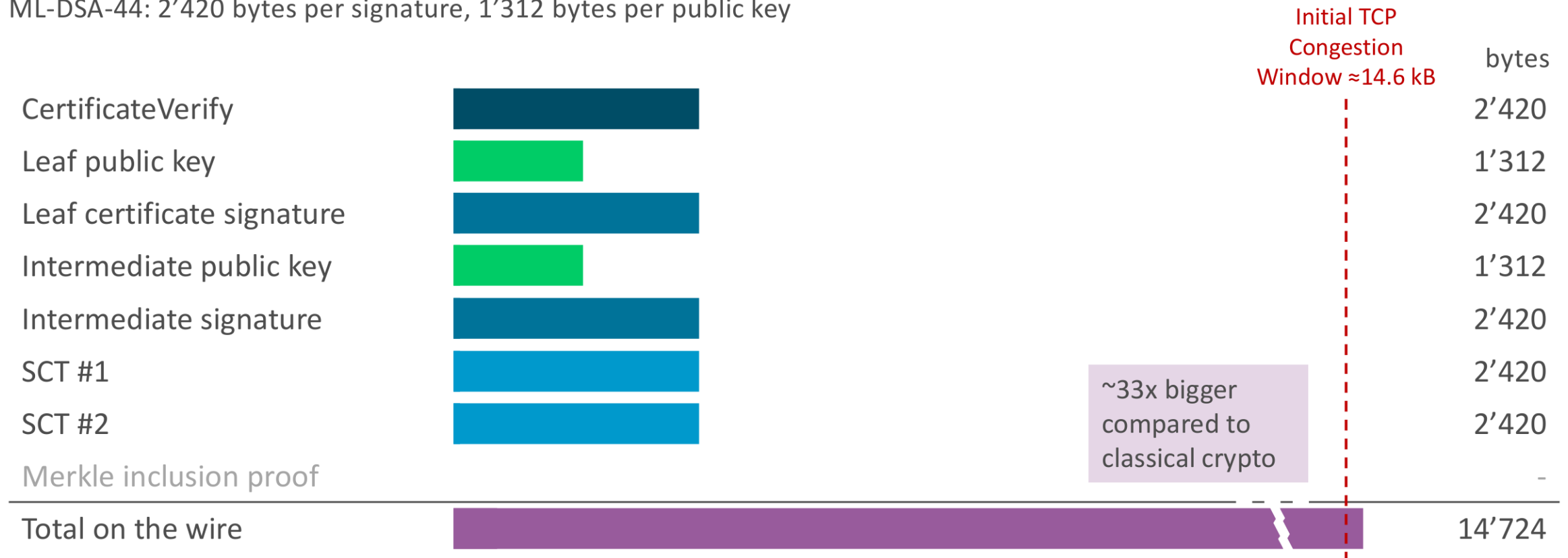
TLS Handshake Size using Classical Cryptography

ECDSA P-256: 64 bytes per signature, 65 bytes per public key



TLS Handshake Size using Post-Quantum Cryptography

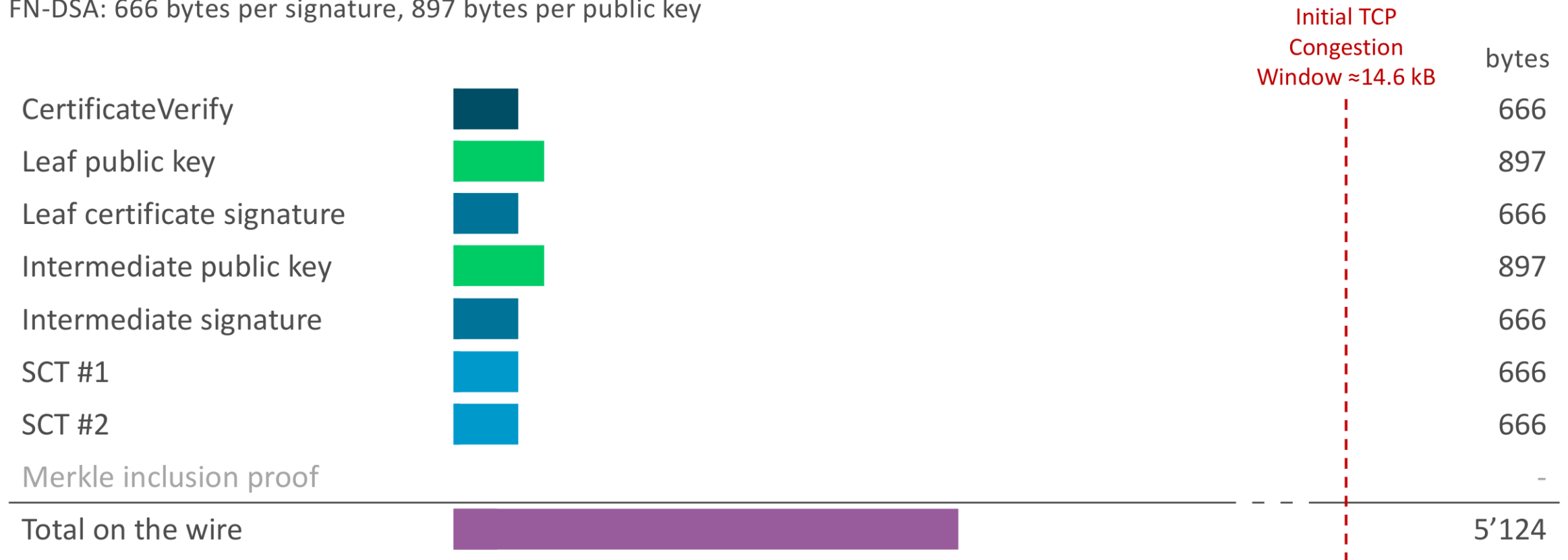
ML-DSA-44: 2'420 bytes per signature, 1'312 bytes per public key



An extra round trip:
The server cannot put 14 kB on the wire
before the first ACK

TLS Handshake Size using Falcon-512

FN-DSA: 666 bytes per signature, 897 bytes per public key



Back under the window, but:

- Computation is more complex and costly
- FN-DSA is not standardised yet

Biggest Weakness of Quantum Signatures?

Their size!

What can we do?

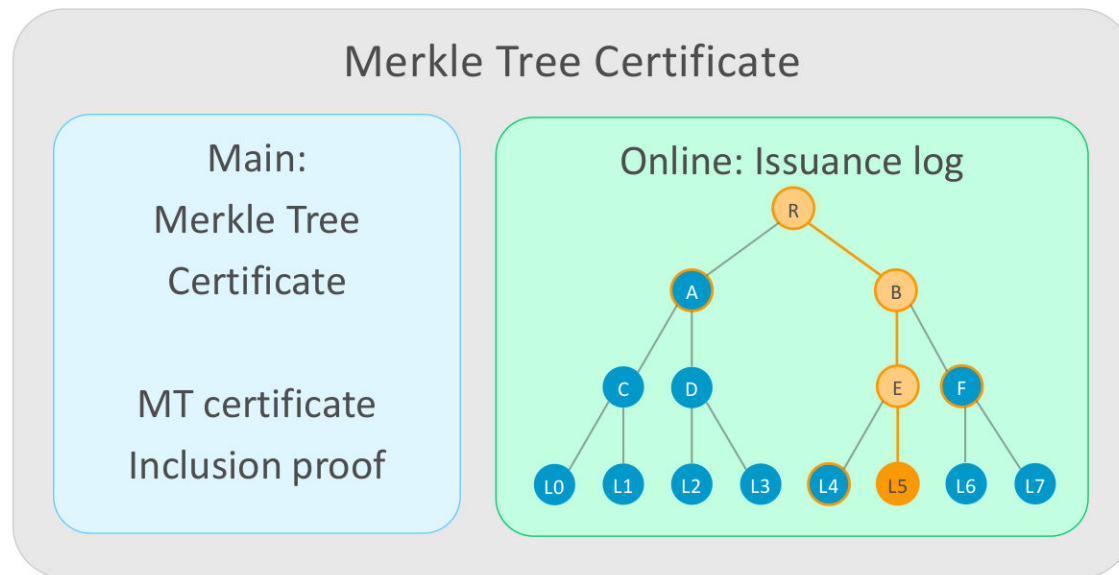
Reduce the size?



Reduce the number
of signatures?

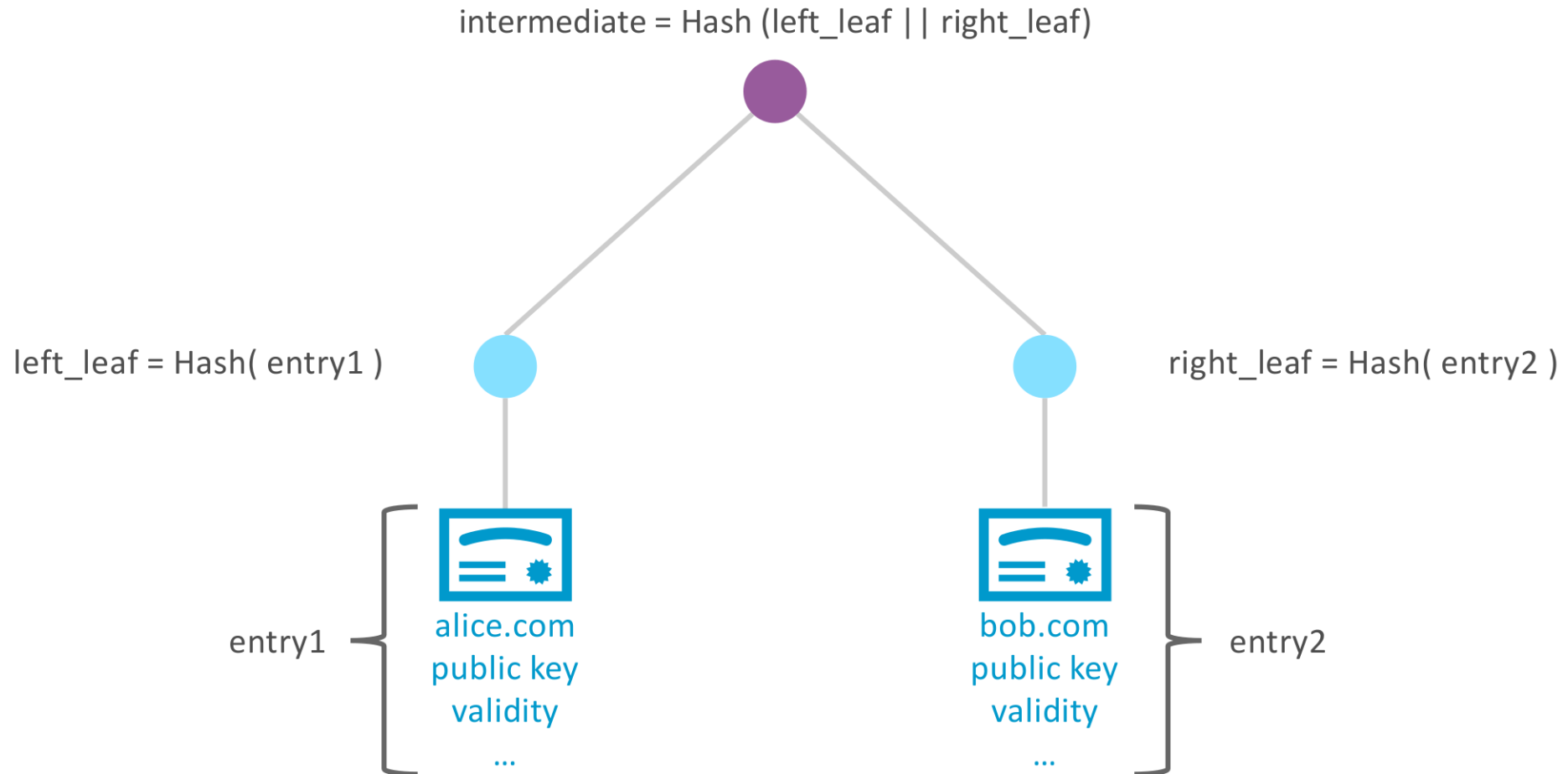


Merkle Tree Certificates



How a Merkle Tree is Built

Distinguishing hashes of entries from intermediate hashes of hashes



Adding More Entries to the Merkle Tree Log

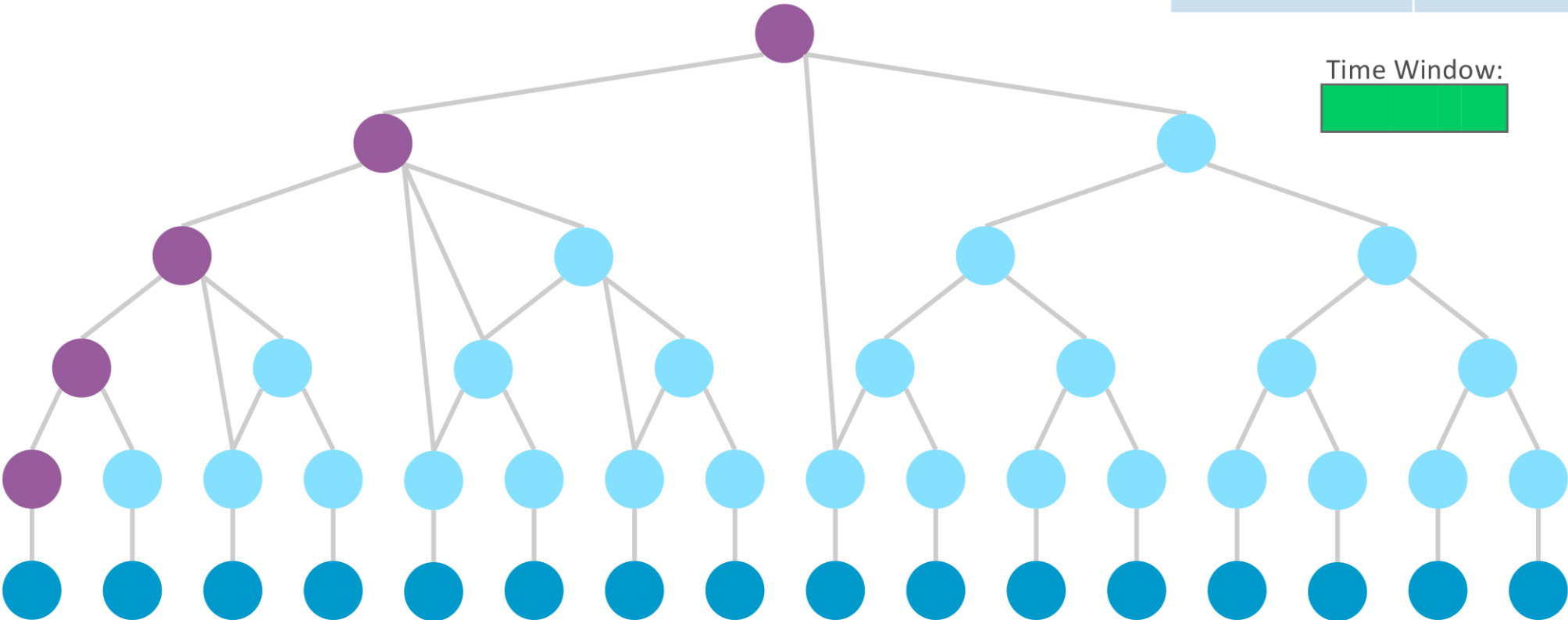
The certificate becomes a path, not a chain

Checkpoint:

Entries	Root Hash
12	0x71..48



Time Window:

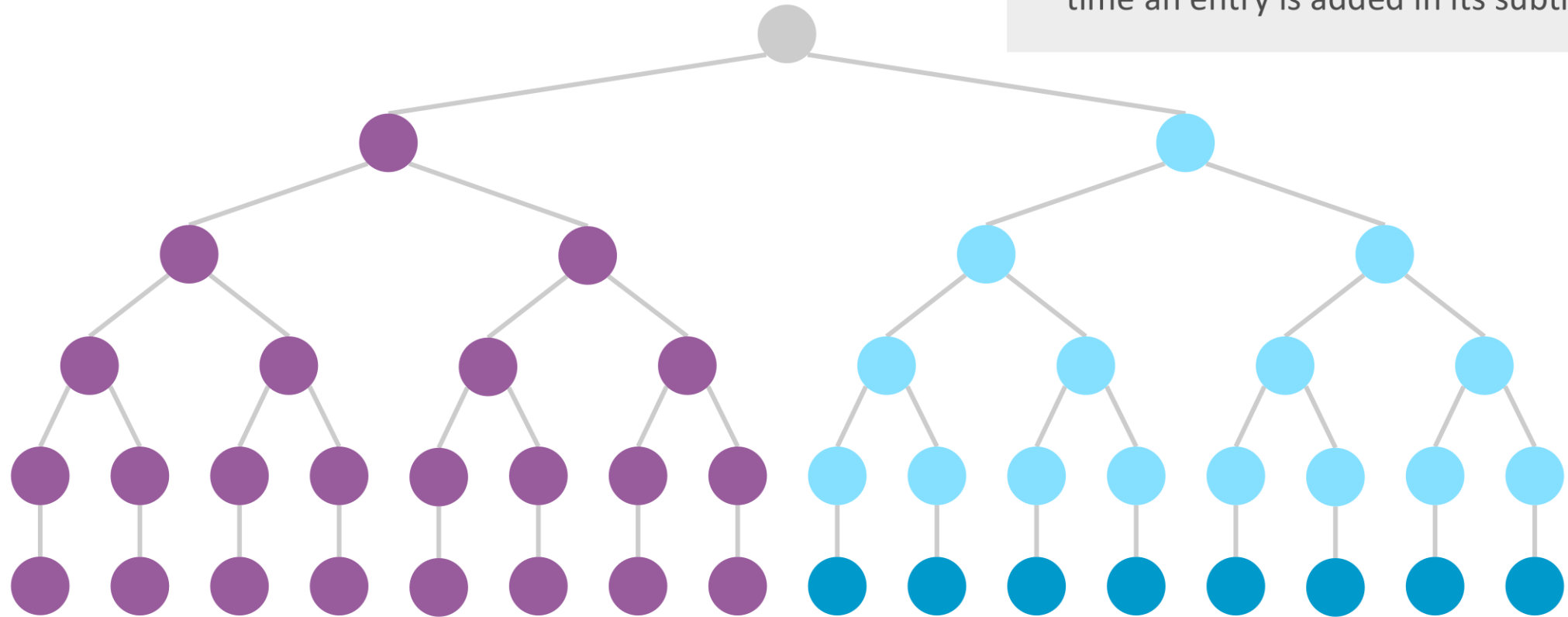


And the log just keeps growing

Once a Branch Is Full, Its Hash Never Changes

New entries only ever touch the right-hand edge of the tree

The root of a branch changes every single time an entry is added in its subtree...



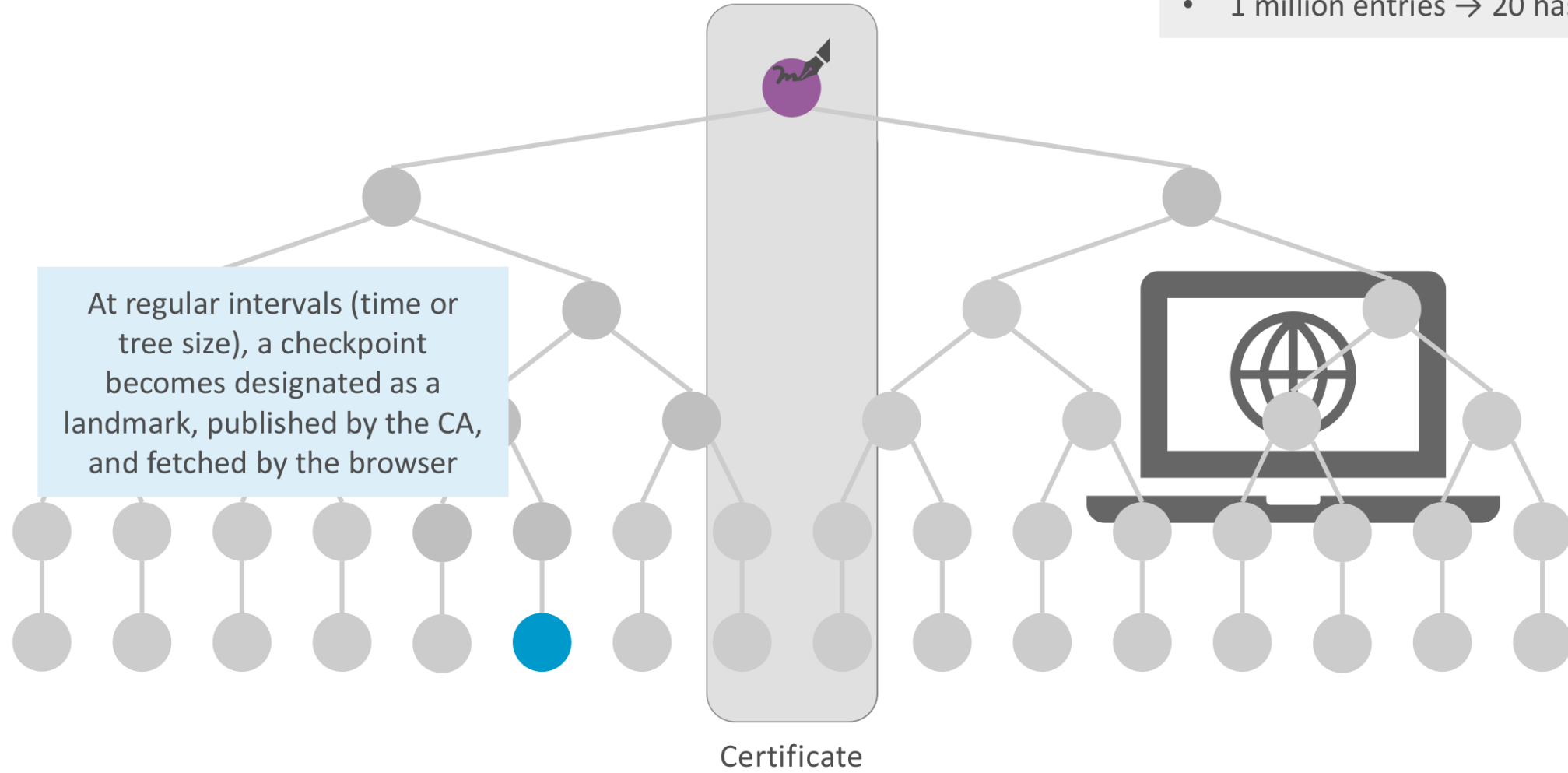
...but once the subtree is full, its root hash value is valid forever

Inclusion Proof

Convince client we can reach the signed root/checkpoint

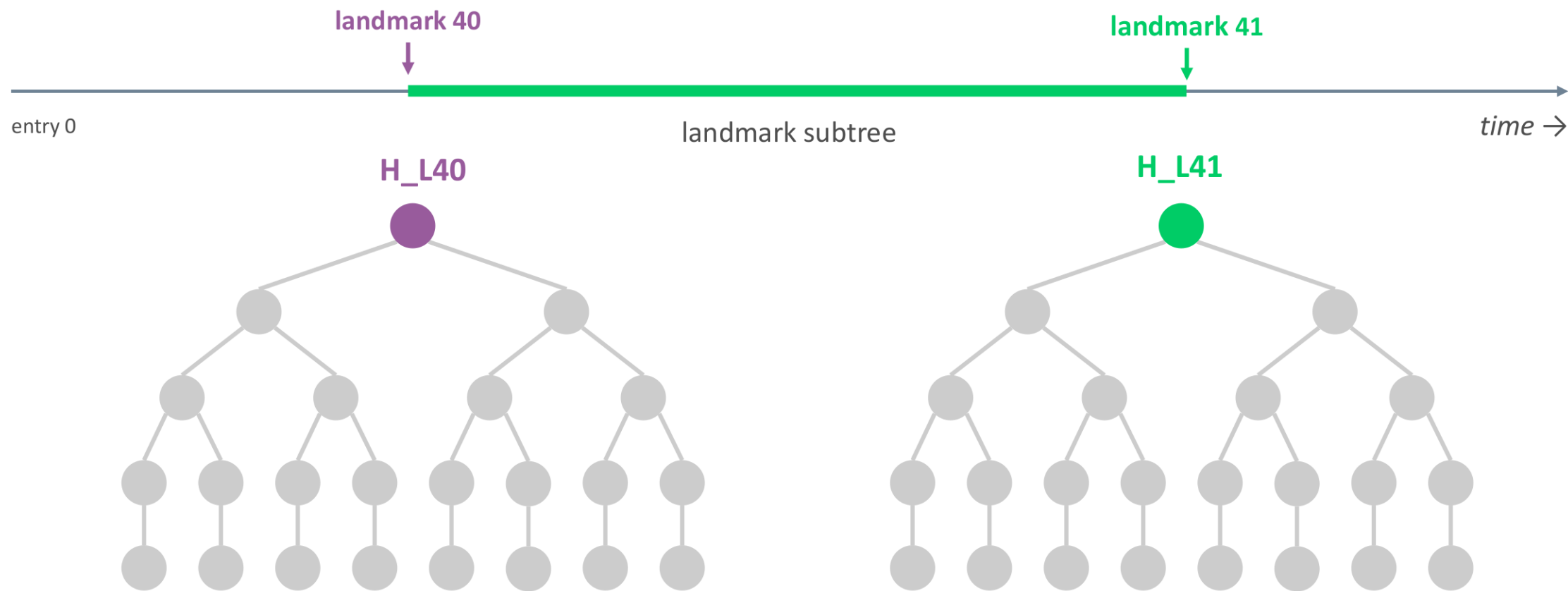
Logarithmic scale:

- 16 entries $\rightarrow$ 4 hashes
- 1 million entries $\rightarrow$ 20 hashes

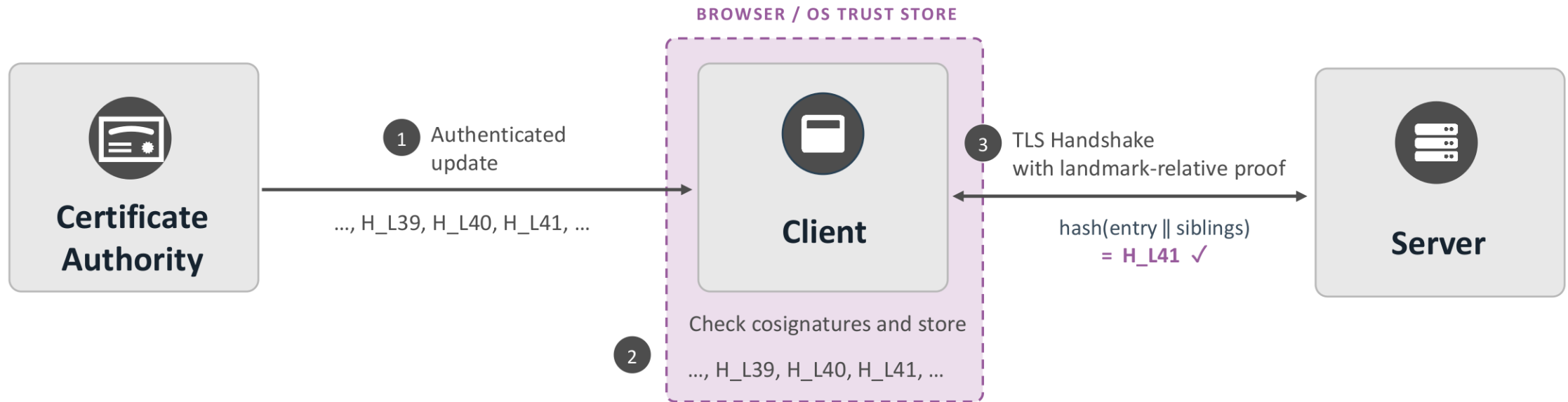


Landmarks

An agreed tree size — and the subtree hash it fixes.



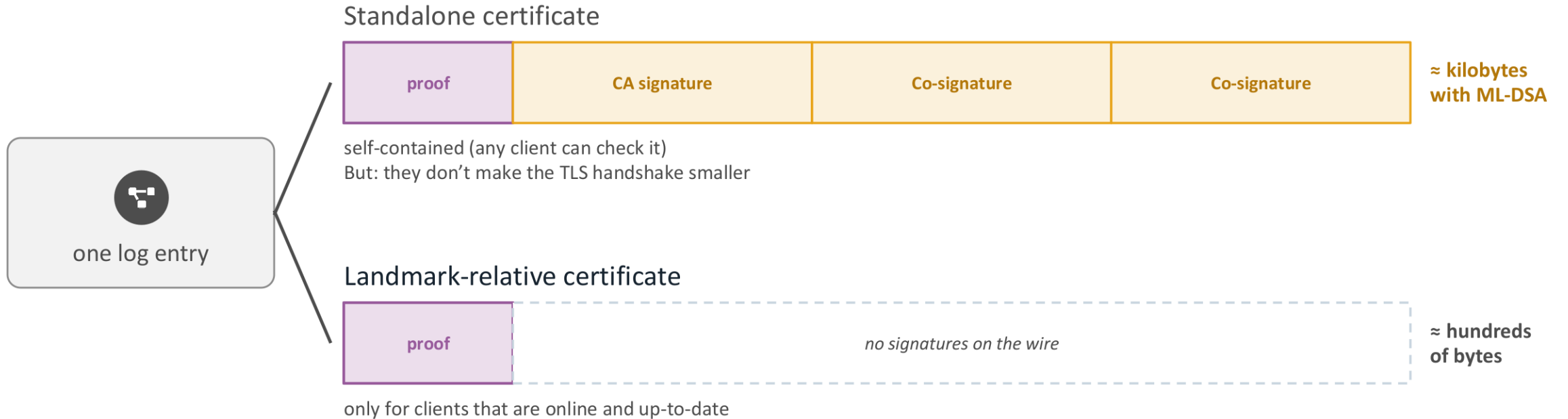
Out-of-band Transmission of Landmarks



Stale client, or not a browser? The server falls back to the full certificate.

Standalone vs. Landmark-relative certificates

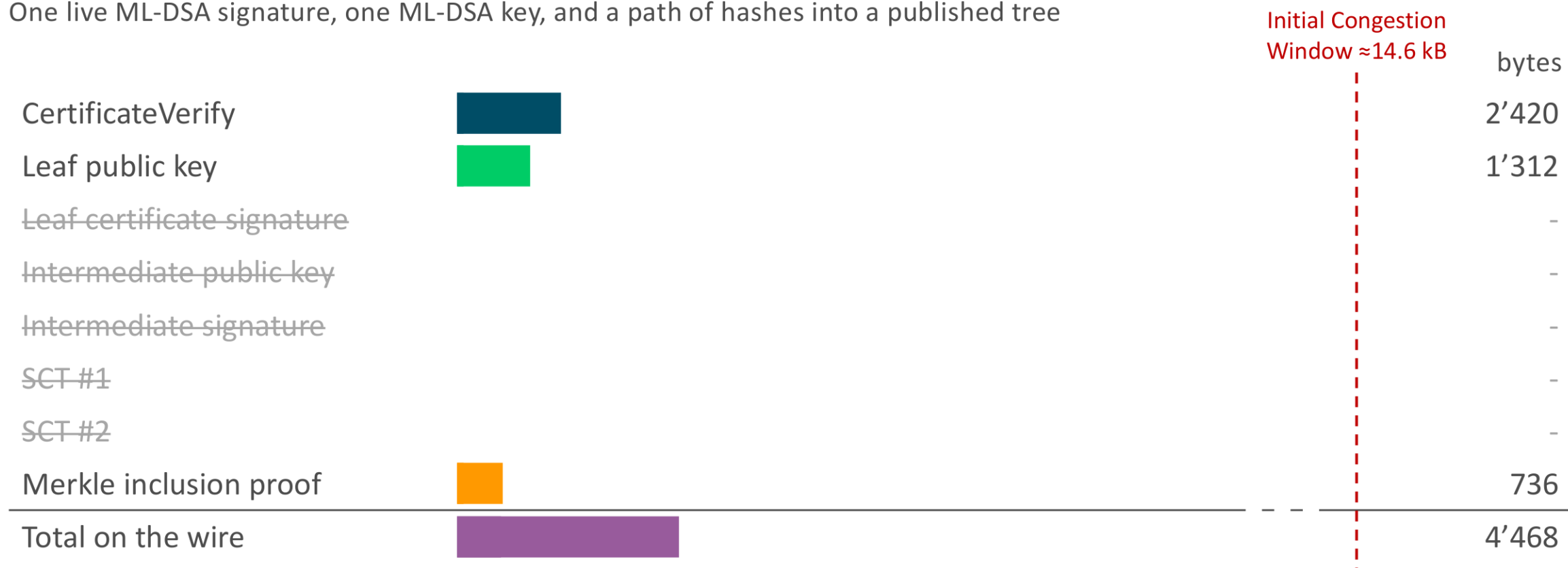
CA signs the tree, not each certificate.



Landmarks have been fetched by the browser using an out of band mechanism.
It validates the landmarks upon fetching → established trust.

TLS Handshake Size using Landmark-relative Certificates

One live ML-DSA signature, one ML-DSA key, and a path of hashes into a published tree



Back under the window with ML-DSA algorithm!

MTC can solve the size issue.

But:

It requires a paradigm shift!

What it costs to use MTC

Smaller handshakes aren't free: four costs to plan for



2×

Certificates per endpoint
Standalone plus landmark-
relative. Forever.



~1 h

New update channel
Landmarks are pushed to
clients out of band, roughly
hourly



10.8 kB

Client state per CA
7-day certs, hourly
landmarks: 169 landmarks,
338 hashes



Draft

Unfinished standard
The OID naming scheme for
CAs, logs and landmarks may
still change

Fewer bytes in the handshake, more moving parts around it

Where do we stand with MTCs?

Google Security

Chrome
Security

Cultivating a robust and efficient quantum-safe HTTPS

Feb 27, 2026 | 4 min read



[Documentation](#) [Get Help](#) [Blog](#) [Donate](#) [About Us](#)

Blog

A Post-Quantum Future for Let's Encrypt

By Andrew Gabbitas · June 3, 2026

Early 2026
Chrome x Cloudflare

Feasibility experiment using 1000 TLS certs live. Cloudflare re-encodes existing certs from trusted CAs as MTCs.

June 2026
Let's encrypt commits to use MTC

Named MTCs as its "way forward" for post-quantum. They issue 54.4% of all public TLS certificates in 2026.

September 2026
Apple will use MTC for server authentication

Apple Root Program policy is being established for MTCs, for Server Authentication only.

Q1 2027
Bootstrap MTC infrastructure

Existing CT log operators are invited to become the first public MTC infrastructure: the issuance logs, cosigners and mirrors.

Summary

What to take away from this talk

01

Post-quantum changes the economics

Simply swapping PQ signatures into today's certificates would degrade performance at Internet scale.

02

The bottleneck is authentication, not encryption

PQ key exchange is already deployed, but five signatures and two public keys blow the size budget.

03

MTCs move the work out of the handshake

Browsers fetch landmark hashes in the background, so a certificate needs only a few hundred bytes of hashes.

04

Transparency is built in

Certificate Transparency becomes a first-party property of issuance, not an add-on.

We don't make signatures smaller.

We remove four out of five from the handshake.

The logo is centered within a purple square. The background of the entire image features three large, concentric dashed circles: a blue one on the left, a grey one in the middle, and a light grey one on the right.

zühlke
empowering ideas