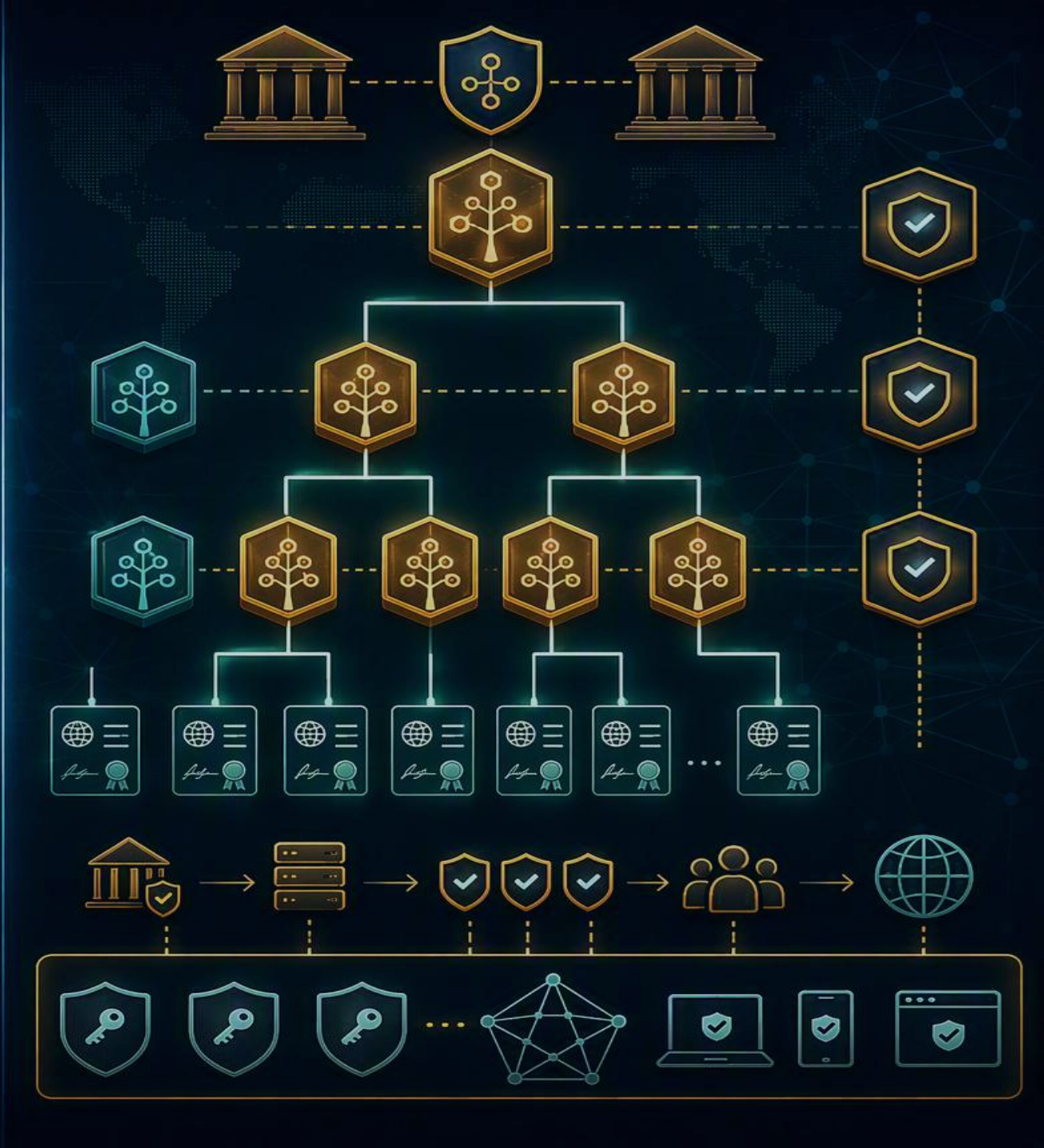
sectigo

The future of TLS certificates



Iñigo Barreira | CA Manager | 2026 – CA Day Tallin

Nowadays

sectigo

TLS is entering a structural transition

Four forces are converging at the same time.

Lifetimes

398 → 200 → 100 → 47 days

Automation

Manual operations stop scaling

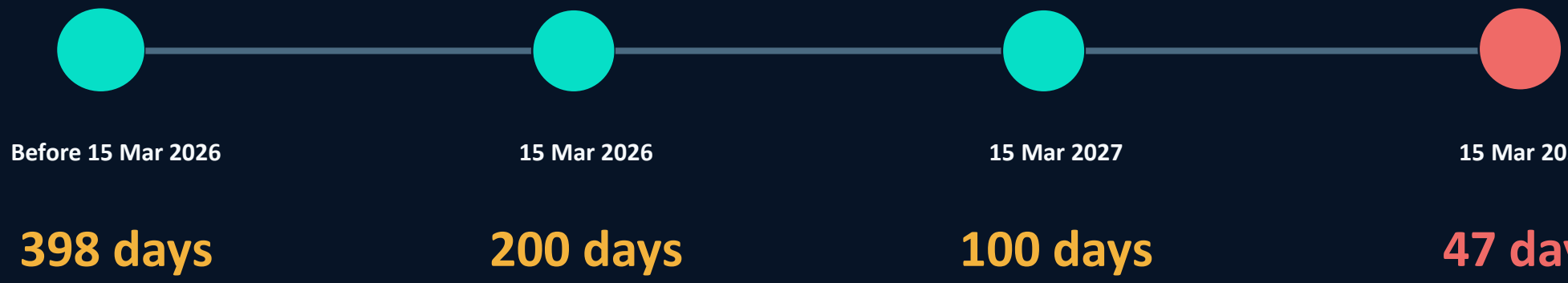
Assurance

More validation (CAA, DNSSEC, …) , linting and resilience

Quantum: new algorithms and potentially new certificate forms

The validity step-down is already the clock

Certificate and validation reuse periods are shrinking in stages.



MTC: 7 days???

47-day TLS makes manual management untenable

The risk shifts from certificate expiry to automation failure.

What multiplies

Renewal events
DCV operations
Deployment changes
Monitoring signals
Exception handling

What must improve

Inventory coverage
ACME integration
Deployment
Rollback
Ownership

Automation is a must: Discover, Issue, Deploy and Renew

The TLS Baseline Requirements keep tightening

Validation evidence, DNS security, legacy methods and operational readiness. CABF TLS ballots during 2026

SC094

DNSSEC exception in email DCV methods

SC096

Carve-out for DNSSEC verification logging requirements

SC097

Sunset all remaining use of SHA-1 signatures in certificates and CRLs

SC095

Clean up

SC099

Improve recording of validation method

SC098

Process RFC 8657 parameters

SC0101

Clarify Authorization Domain Names

SC100

DNSSEC Clarification and Consolidation

clientAuth EKU removal is a browser decission

Validation is becoming more distributed and reproducible

Reduce single-perspective and weakly evidenced issuance decisions.



Future-proof issuance needs observable evidence at every gate.

Revocation is also being redesigned

Toward scalable and privacy-preserving distribution.

OCSP pressure

Privacy leakage
Network round trips
Soft-fail behavior
Responder cost and availability

AIA optional (SC-104)

CRL evolution

Mandatory CRLs
Partitioning
Browser aggregation
Efficient distribution

Short-lived future

Less useful status checking
More reliance on automation
Incident response still matters

No revocation

Certificate profiles will become more specialized

Dedicated hierarchies, constrained EKUs and cleaner policy boundaries.

Dedicated trust

Separate TLS, S/MIME, code-signing and other hierarchies

Tighter purpose

Constrained EKUs, profiles and intended relying-party use

Cleaner governance

Fewer multi-purpose CAs and less accidental coupling

Quantum changes the certificate signature problem

Certificate authentication has harder deployment trade-offs than key establishment.

Key establishment

Hybrid KEMs can protect confidentiality without replacing certificate signatures.

Certificate signatures

ML-DSA and other PQ signatures increase key, signature and chain sizes.

Trust distribution

Roots, clients, logs, HSMs, profiles and audits must evolve together.

The PQC dilemma

Classic PQC or MTC

sectigo

Path A: traditional PQC in X.509

Keep the familiar chain model, replace or combine signature algorithms.



PQ root

PQ intermediate

PQ leaf

TLS server

PQ-capable client

Strength

Continuity with existing PKI, audit and tooling

Cost

Larger certificates and signatures, plus CT and compatibility work

Microsoft’s pilot: traditional PQC hierarchies

Closed testing of ML-DSA certificates, tooling and compatibility.



What it enables

Pilot CAs and test roots using regular PQC hierarchies

What it measures

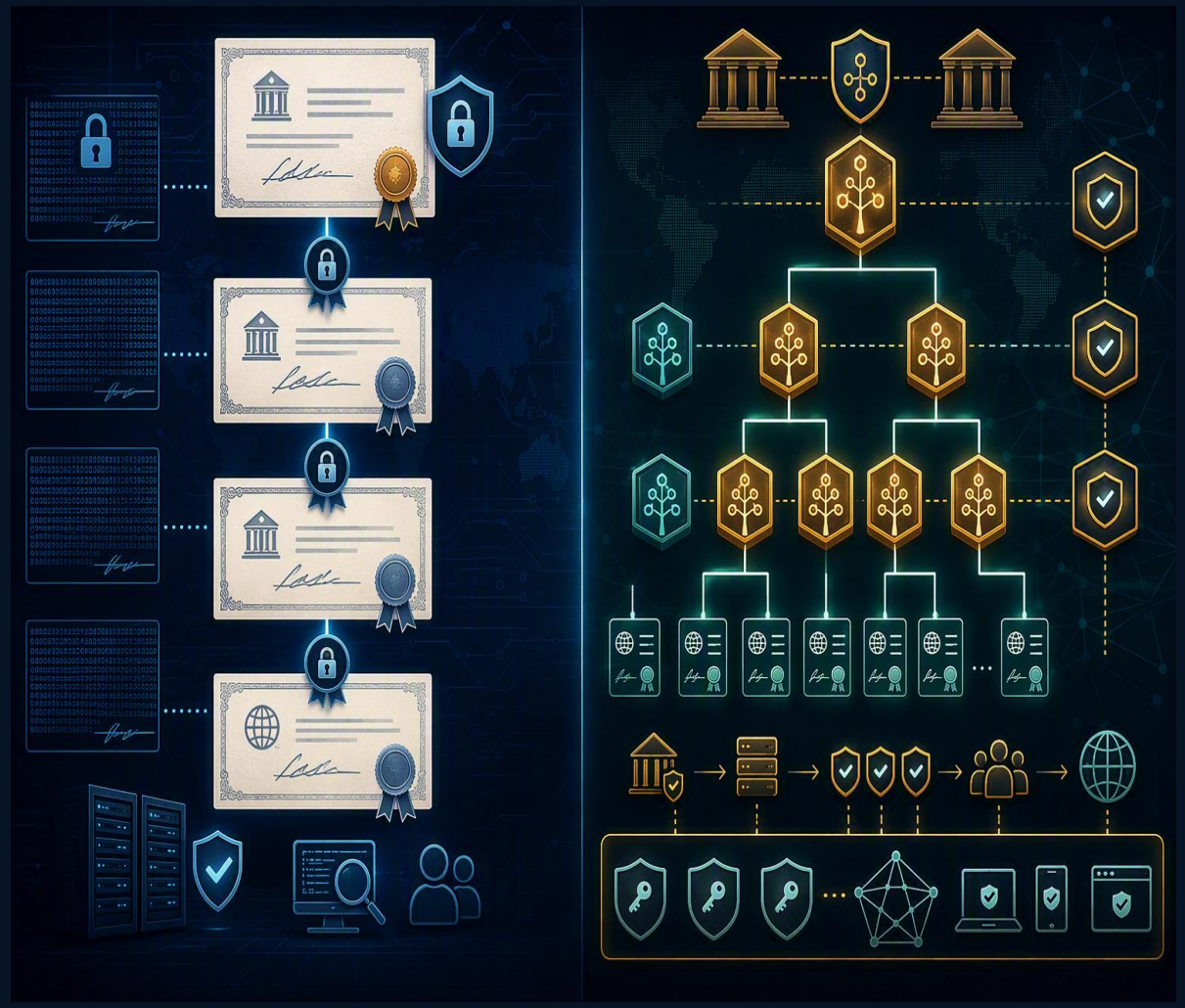
Compatibility gaps across workflows, applications and policies

What it does not mean

Public WebPKI acceptance or a final production profile

Path B: Merkle Tree Certificates

Move repeated authentication cost into logged commitments and checkpoints.



Integrated issuance

CA appends issuance data and signs tree checkpoints

Two forms

Standalone first; smaller landmark form after a checkpoint

New dependencies

Mirrors, cosigners, fresh trust material and MTC-aware clients

Chrome’s draft quantum-resistant program chooses MTC

A separate trust ecosystem for MTC CAs and mirroring operators. Stage 1 ongoing started with TSPs that currently offer a CT log

Separate trust store

Distinct from the existing Chrome Root Store and CT ecosystem.

Two operator classes

MTC CA Operators maintain trees; Mirroring Operators replicate and cosign.

Policy-based assurance

Lifecycle, linting, log integrity, availability, audits and incidents.

MTC vs traditional PQC X.509

The key question is where complexity and repeated cost live.

Authentication	Inclusion proof + checkpoints	Per-certificate PQ signature
Handshake	Lower repeated overhead	Large keys/signatures in chain
Transparency	Integrated	Separate CT layer
Compatibility	New trust model	Familiar X.509, new algorithms
Operations	Trees, mirrors, cosigners	CA hierarchy, CT, status
Migration	Parallel MTC and legacy	Algorithm or hybrid transition

Evolution

How is this affecting the current DV, OV, EV and QWACs?

sectigo

The CA operating model must evolve

Assurance spans policy, automation, log integrity and resilience.

Policy

CP/CPS, profiles, algorithm and key agility

Validation

DCV, MPIC, CAA, DNSSEC, evidence

Issuance

Linting, HSMs, trees or PQ signatures

Delivery

ACME, alternate artifacts, telemetry

Resilience

Mass revocation, mirrors, rollback

Audit

Cryptographic and operational evidence

The transition does not affect every TLS product equally

The common cryptographic and lifecycle pressure is the same; identity and regulatory dependencies change the solution.



DV is the easiest product to industrialise

Its assurance is domain control, so the primary challenge is resilient renewal and deployment rather than identity revalidation.

What changes

- Renewal frequency rises sharply
- DCV evidence becomes short-lived
- PQC may enlarge chains
- MTC requires new client trust logic

Best-fit solution

- ACME by default
- Persistent or delegated DNS validation where permitted
- Inventory + endpoint ownership
- Atomic deployment and rollback

Strategic role

- Default transport certificate
- First product for PQC pilots
- Natural companion to separate identity credentials
- Lowest-cost path to high-frequency issuance

OV and EV need two automation loops

Short-lived domain credentials and longer-lived verified identity should be managed separately, then bound at issuance.

1. **Pre-validate identity**
2. **Authorise requesters**
3. **Automate DCV**
4. **Issue + deploy**

OV: automate around reusable organisation data

- Maintain a governed organisation identity record
- Bind authorised requesters or accounts to that record
- Refresh domain control at required cadence
- Revalidate only when data age or change requires it

EV: preserve due diligence, automate the hand-offs

- Keep the EV verification corpus and independent review
- Automate request authentication, evidence routing and linting
- Separate approval from repetitive deployment
- Pilot PQ profiles without weakening EV semantics

QWACs need an explicit architecture decision

A QWAC that remains publicly trusted inherits WebPKI lifecycle and profile constraints; qualified use may justify separation.

Option 1: 1 -QWAC

- One certificate carries TLS and qualified identity
- Follows TLS BR lifetime and DCV cadence
- Needs ACME-compatible identity authorisation
- PQC/MTC profile must align with ETSI, supervision and browsers

Option 2: 2 -QWAC

- DV certificate protects the TLS channel
- Separate qualified certificate conveys organisation identity
- Reduces coupling between rapid TLS rotation and qualified identity
- Requires secure binding and relying-party support

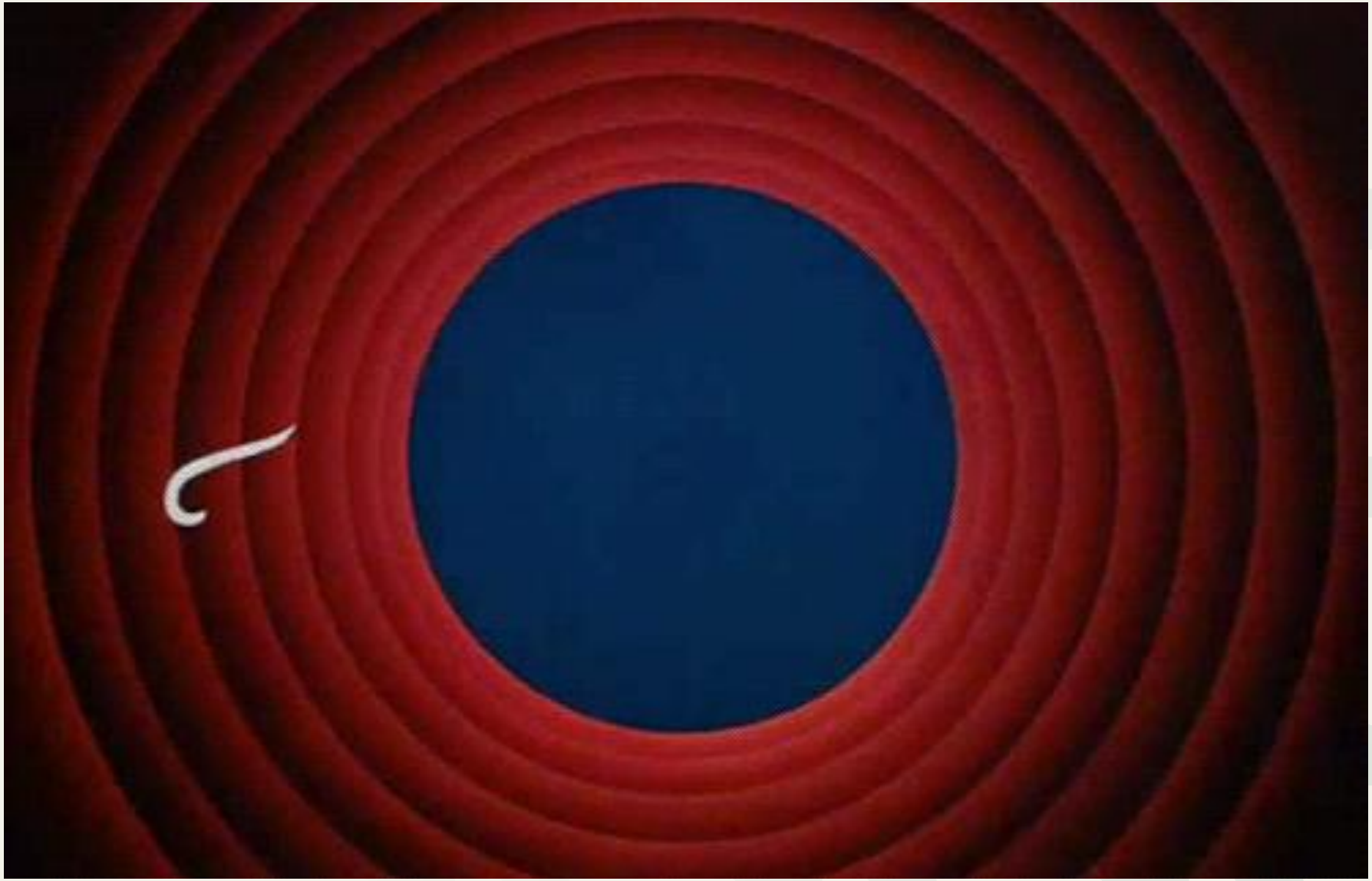
Option 3: EUTL-only qualified path

- Qualified certificate moves outside browser WebPKI
- Longer validity or clientAuth can follow the qualified profile
- Public serverAuth remains a separate DV, OV or EV certificate
- Requires dedicated hierarchy, audit and transition governance

Five conclusions

Shorter-lived, automated, better evidenced and eventually quantum-resistant.

1. **Automation is mandatory infrastructure: ACME**
2. **Validation and evidence will keep tightening: CAA, DNSSEC, linting, profiles, …**
3. **Revocation and hierarchy models will simplify: Short-lived certificates do not need CRL/OCSP**
4. **MTC and traditional PQC parallel pilots: PQC adds size and compatibility, MTC adds a new ecosystem (can all CA/TSPs handle a MTC solution?)**
5. **Crypto-agility matters**



sectigo