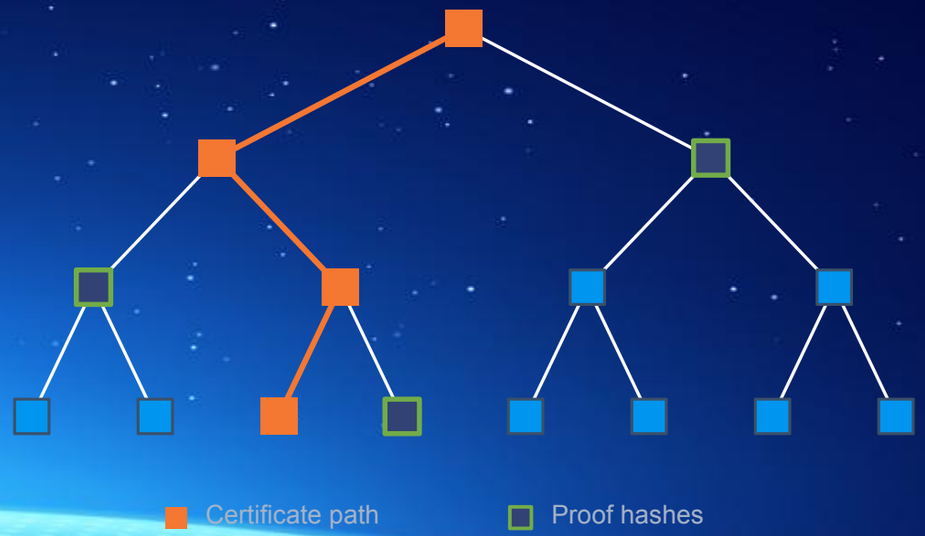
Next-Generation WebPKI

Towards Post-Quantum Trust with MTCs

TrustAsia | Alison Wang



亞洲誠信® TRUSTAsia

The Path to Post-Quantum WebPKI

01

Why Merkle Tree Certificates Matter

02

Migration to Post-Quantum WebPKI

03

TrustAsia in the MTC Ecosystem

04

Preparing Your Organization for PQC

01

Why Merkle Tree Certificates Matter

Quantum Threats Strike Public-Key Trust and Key Exchange First

Current Algorithms in Digital Certificates & TLS

Algorithm Type	Common Algorithms	Quantum Impact
Digital Signature (Asymmetric)	RSA / ECDSA	Critical
Key Exchange (Asymmetric)	ECDHE / RSA	Critical
Symmetric Encryption	AES / ChaCha20	Manageable
Hash Function	SHA-256 / SHA-384	Minimal

Direct Impacts

01 Forged Trust Chains

02 Retroactive Decryption (HNDL)

03 Ecosystem-Wide Migration

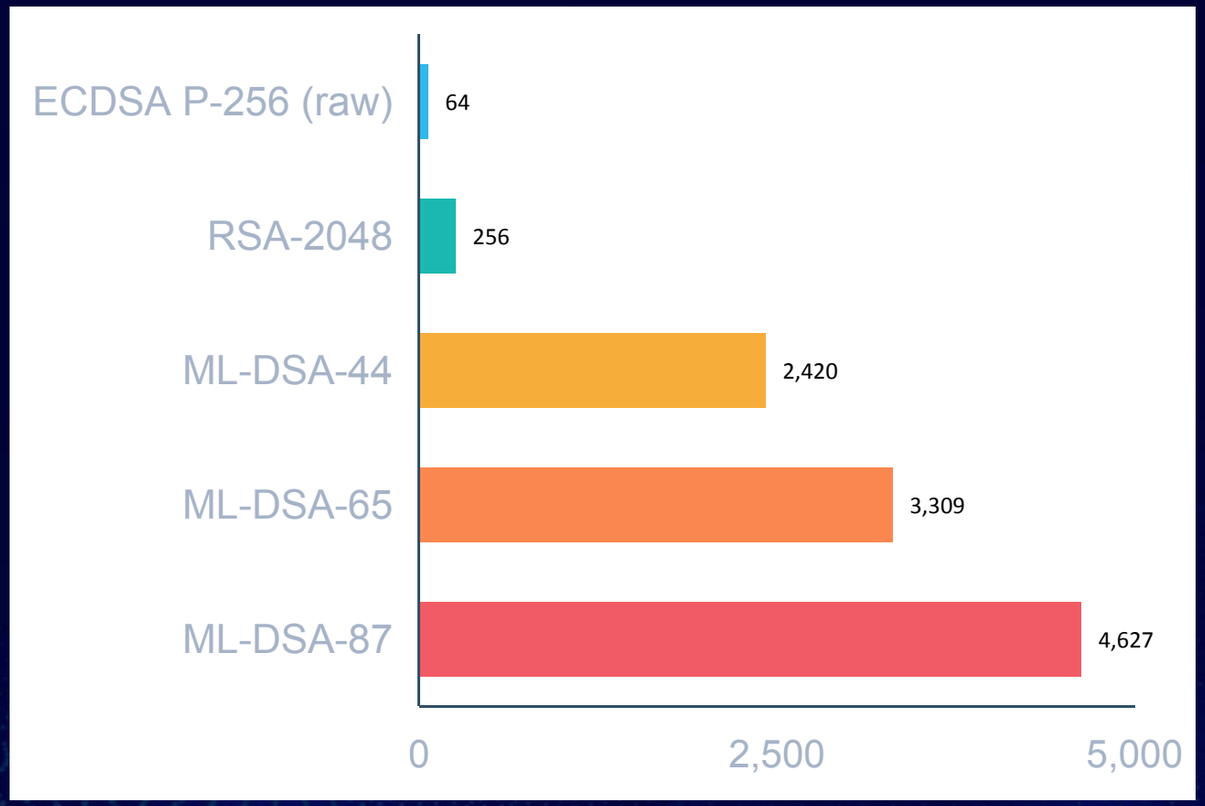
HTTPS | eID | eInvoice

eSigning | IoT | Software Signing

亞洲誠信® TRUSTASIA

How Much Larger Are Post-Quantum Signatures?

Single-signature size, in bytes



3,309 bytes

One ML-DSA-65 signature

Authentication gets larger

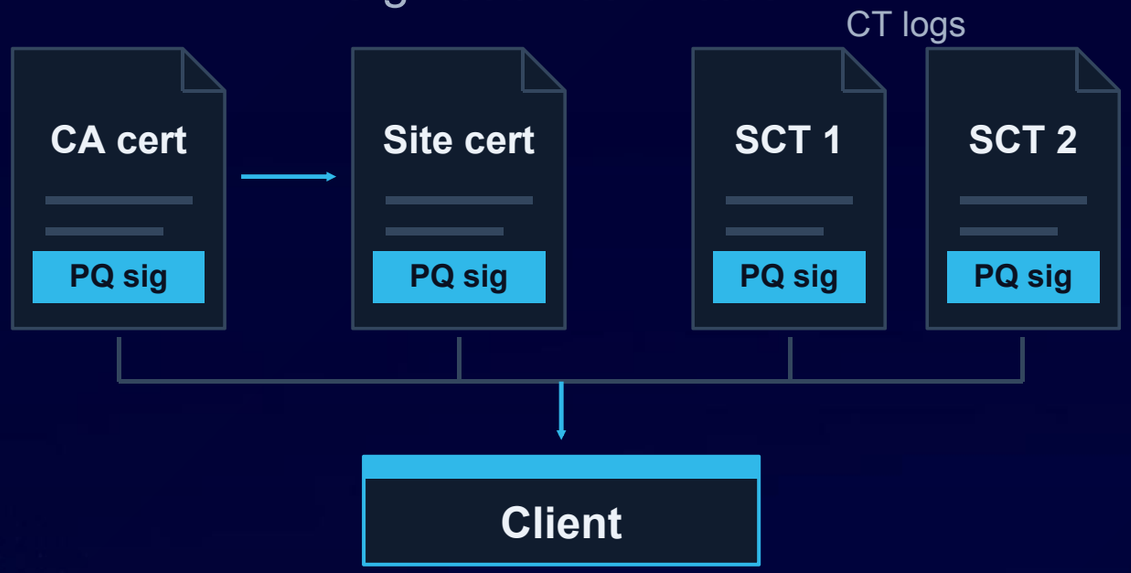
Infrastructure bears the cost

亞洲誠信® TRUSTAsia

Choosing a PQC Migration Path for WebPKI

Traditional X.509

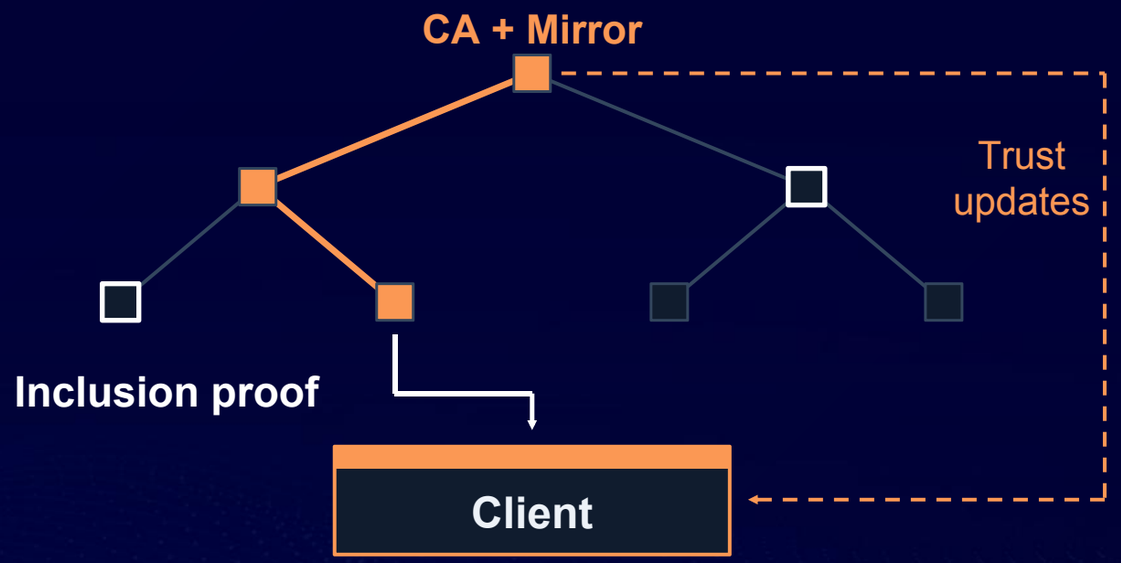
Sign each certificate

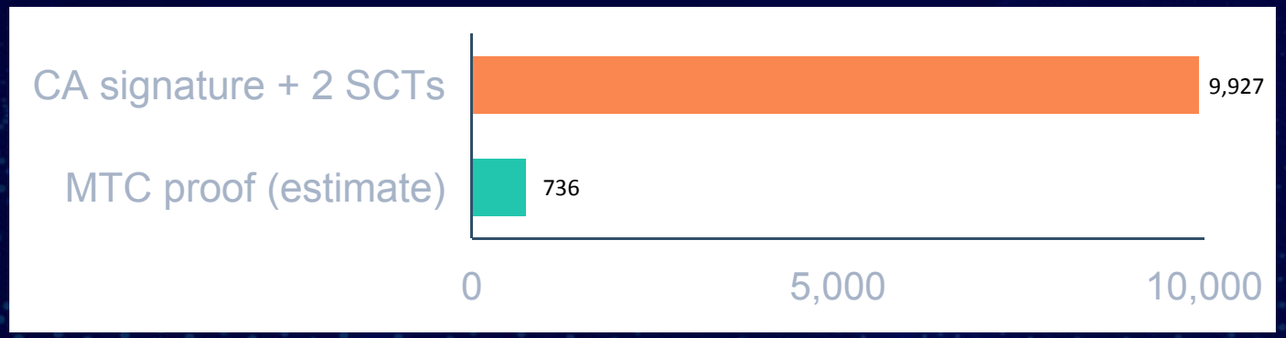


vs

MTCs

Authenticate a shared subtree





- **Transparency at issuance**
- **Signatures move out of band**

亞洲誠信® TRUSTAsia

Trust Distribution Connects Design to Deployment

Landmark-relative

Certificate sent by the server

- Identity + public key
- Inclusion proof

Client

Verify the proof against a trusted subtree

Trusted subtree already on the client

Standalone

Certificate sent by the server

- Identity + public key
- Inclusion proof
- CA / Mirror cosignatures

Client

Verify the proof and included cosignatures

亞洲誠信® TRUSTAsia

Certificate Structure: 25.5 KB to 2.7 KB



Remove three external SCTs	−9.9 KB
Omit transition cross-certificate	−3.5 KB
Omit intermediate chain	−6.0 KB
Replace leaf signature & simplify fields	−3.3 KB
Retain key, proof & identity	≈2.7 KB

亞洲誠信® TRUSTAsia

Participants in the MTC Ecosystem



Implementations are converging

- **Clients and platforms**

Google, Apple, Microsoft / Edge

- **CAs and service operators**

DigiCert, Sectigo, TrustAsia, Let’s Encrypt, Cloudflare

- **TLS software**

OpenSSL

亞洲誠信® TRUSTAsia

02

Migration to Post-Quantum WebPKI

Chrome’s Phased Migration Plan

optimistic and tentative

2027 H1

First MTC CAs

From current CT log operators

→

2027 H2

Other organizations

Embedded PQ opt-out certificates
Limited PQ HSTS support

→

2028 H1

Transition testing

Encourage CAs to test embedded
PQ opt-out certificates

→

2028 H2

Default trust migration

Stated goal: remove non-MTC CAs

From “supporting MTCs” to “requiring a new CA authentication path”.

亞洲誠信® TRUSTAsia

Apple and Microsoft: MTC Plans

Apple: MTC policy for server authentication

By late October 2026

Expected policy draft

Open for public comment

Late summer 2027

Expected CA applications

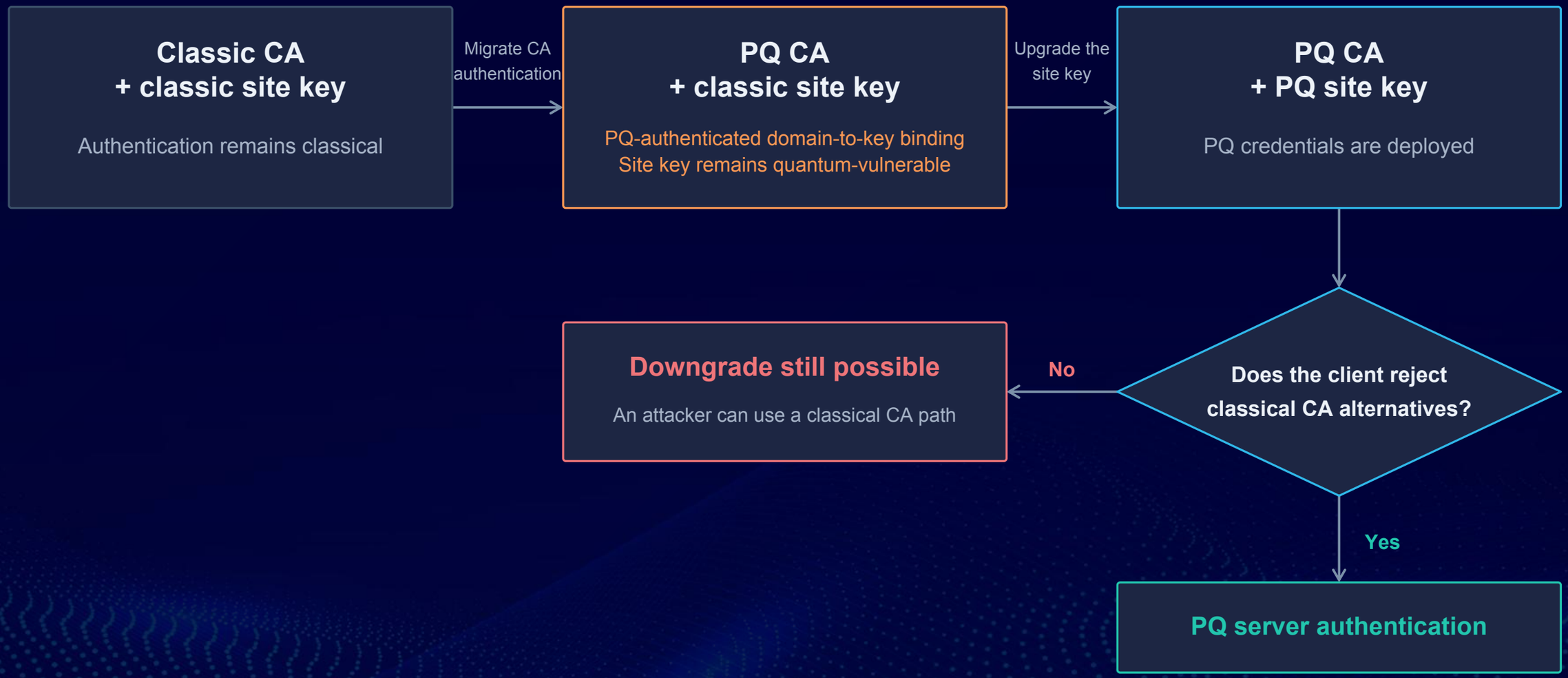
A separate test phase is possible

Microsoft: relying-party support

Windows is evaluating MTC verification. Edge plans to align with Chromium’s implementation and verification timeline, using a Microsoft MTC trust list.

亞洲誠信® TRUSTAsia

Compatibility and Security During Migration



Post-quantum opt-out certificate

Formerly discussed as “Turducken” -- Chrome

Close the classical-CA downgrade path while supporting legacy systems

Classic X.509 outer layer

Verified by legacy clients

Embedded Standalone MTC

PQ authentication for updated clients

Both layers bind the same domain, key P, and validity constraints.

- **Legacy server**

Keep the classical private key and send a compatibly packaged credential.

- **Legacy client**

Verify the classical outer certificate for compatibility.

- **Updated client**

Verify the PQ-authenticated binding, then verify the handshake with P.

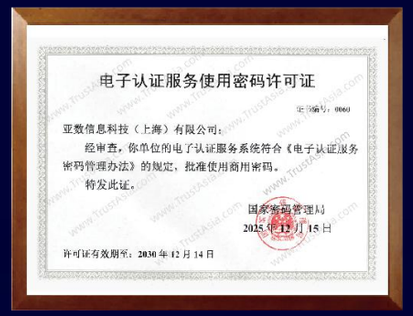
An unforgeable, PQ-authenticated opt-out lets CAs migrate first.

亞洲誠信® TRUSTAsia

03

TrustAsia in the MTC Ecosystem

TrustAsia CA Qualifications: China & International







State Encryption Administration

License for Use of Cipher Codes for Electronic Certification Services

License for Qualifications for E-government Electronic Authentication Service Institutions

China MIIT Certification

License for Electronic Certification Services



WebTrust Accredited

WebTrust seals for Certification Authority, BR-SSL, Extended Validation, Code Signing, Network Security, S/MIME and Mark Certificate

亞洲誠信® TRUSTAsia

One of the World's Eight CT Log Service Providers

Being **the only Asian service provider** among the eight Certificate Transparency Log Operators, together with Cloudflare, DigiCert, GEOMYS, Google, Let's Encrypt, Sectigo and IPng Networks.

TrustAsia offers CT Log services with high availability and stability, hence devoted to helping guarantee compliance, transparency and robust development of the Web PKI community.

亞洲誠信® TRUSTAsia

CLOUDFLARE

digicert®

GEOMYS

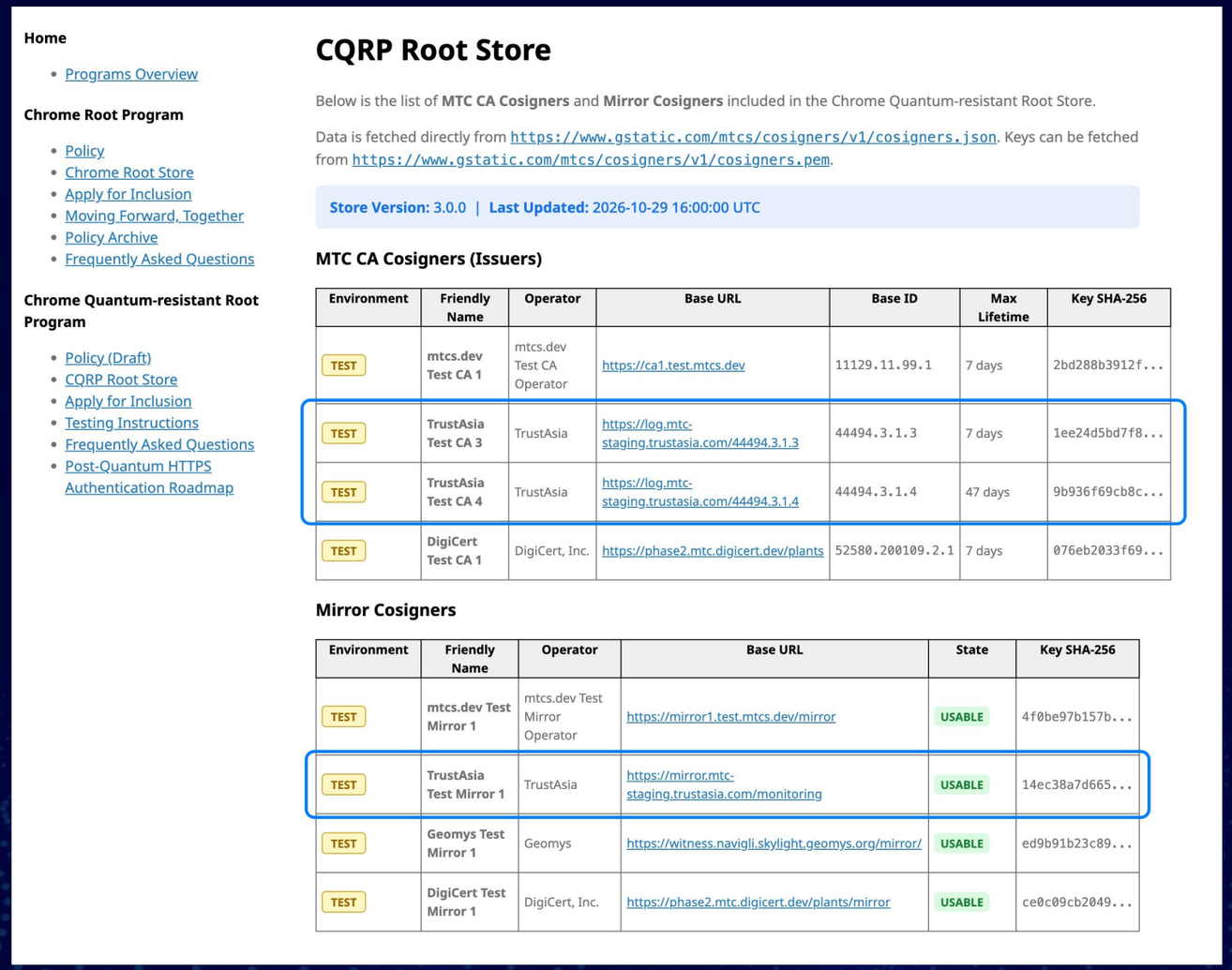
Google

Let's Encrypt

SECTIGO

IPng Networks

TrustAsia MTC Root Inclusion by Chrome



Home

- Programs Overview

Chrome Root Program

- Policy
- Chrome Root Store
- Apply for Inclusion
- Moving Forward, Together
- Policy Archive
- Frequently Asked Questions

Chrome Quantum-resistant Root Program

- Policy (Draft)
- CQRP Root Store
- Apply for Inclusion
- Testing Instructions
- Frequently Asked Questions
- Post-Quantum HTTPS Authentication Roadmap

CQRP Root Store

Below is the list of **MTC CA Cosigners** and **Mirror Cosigners** included in the Chrome Quantum-resistant Root Store.

Data is fetched directly from `https://www.gstatic.com/mtcs/cosigners/v1/cosigners.json`. Keys can be fetched from `https://www.gstatic.com/mtcs/cosigners/v1/cosigners.pem`.

Store Version: 3.0.0 | **Last Updated:** 2026-10-29 16:00:00 UTC

MTC CA Cosigners (Issuers)

Environment	Friendly Name	Operator	Base URL	Base ID	Max Lifetime	Key SHA-256
TEST	mtcs.dev Test CA 1	mtcs.dev Test CA Operator	https://ca1.test.mtcs.dev	11129.11.99.1	7 days	2bd288b3912f...
TEST	TrustAsia Test CA 3	TrustAsia	https://log.mtc-staging.trustasia.com/44494.3.1.3	44494.3.1.3	7 days	1ee24d5bd7f8...
TEST	TrustAsia Test CA 4	TrustAsia	https://log.mtc-staging.trustasia.com/44494.3.1.4	44494.3.1.4	47 days	9b936f69cb8c...
TEST	DigiCert Test CA 1	DigiCert, Inc.	https://phase2.mtc.digicert.dev/plants	52580.200109.2.1	7 days	076eb2033f69...

Mirror Cosigners

Environment	Friendly Name	Operator	Base URL	State	Key SHA-256
TEST	mtcs.dev Test Mirror 1	mtcs.dev Test Mirror Operator	https://mirror1.test.mtcs.dev/mirror	USABLE	4f0be97b157b...
TEST	TrustAsia Test Mirror 1	TrustAsia	https://mirror.mtc-staging.trustasia.com/monitoring	USABLE	14ec38a7d665...
TEST	Geomys Test Mirror 1	Geomys	https://witness.navigli.skylight.geomys.org/mirror/	USABLE	ed9b91b23c89...
TEST	DigiCert Test Mirror 1	DigiCert, Inc.	https://phase2.mtc.digicert.dev/plants/mirror	USABLE	ce0c09cb2049...

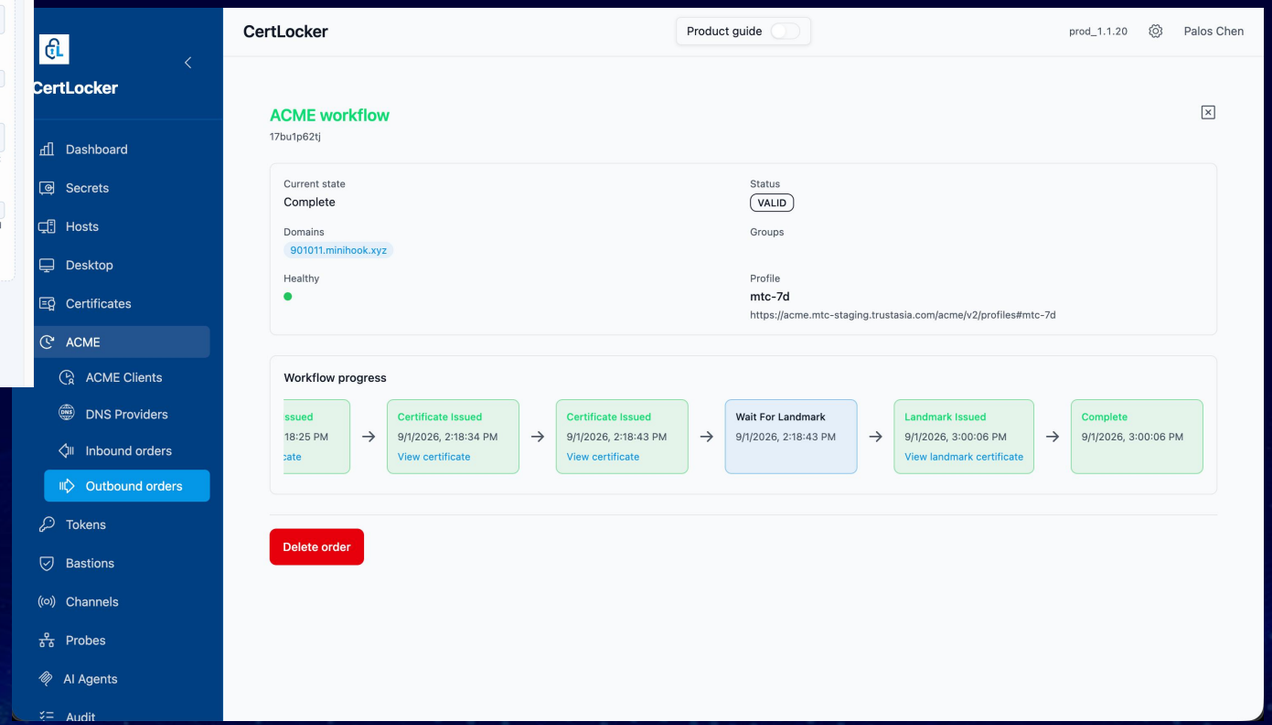
- TrustAsia has been included in the Chrome Quantum-resistant Root Store as
  - MTC CA Cosigners
  - Mirror Cosigners

亞洲誠信® TRUSTASIA

TrustAsia MTC Progress and Achievements



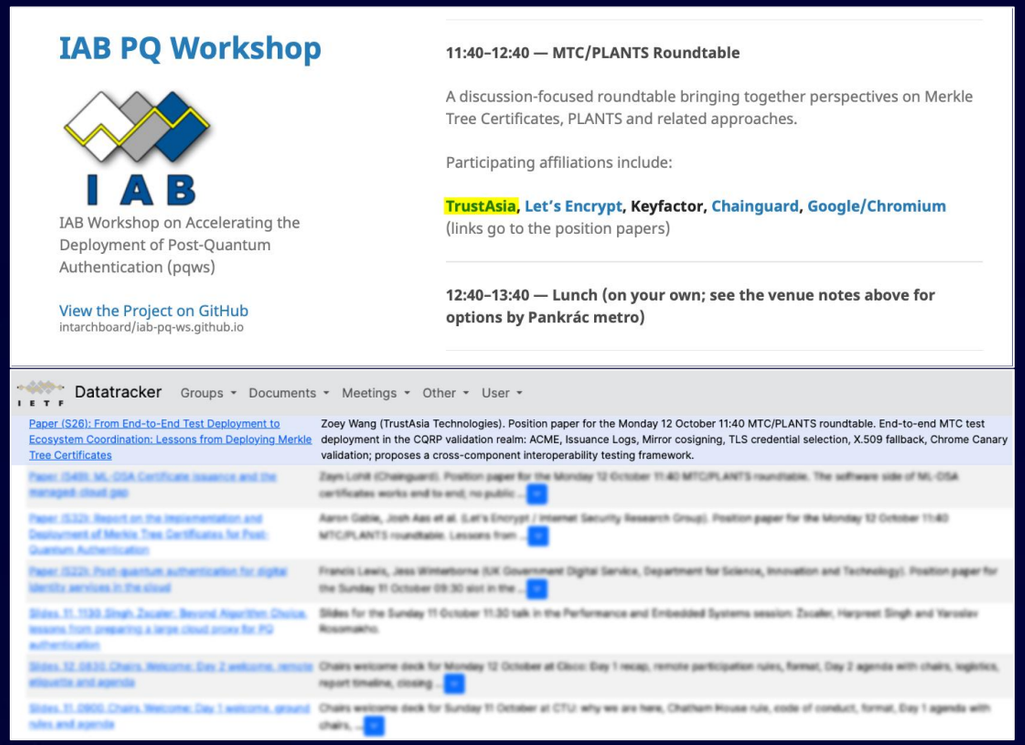
- TrustAsia–issued MTCs validate in Chrome Canary with the required MTC test features enbaled. (Try it now ➡ https://mtcdemo.trustasia.cn)



- TrustAsia's ACME server has completed interoperability testing with the CertLocker ACME client, successfully issuing trusted MTC certificates.

亞洲誠信® TRUSTAsia

TrustAsia Active Participation in MTC Standardization



IAB PQ Workshop

IAB

IAB Workshop on Accelerating the Deployment of Post-Quantum Authentication (pqws)

View the Project on GitHub
intarchboard/iab-pq-ws.github.io

11:40–12:40 — MTC/PLANTS Roundtable

A discussion-focused roundtable bringing together perspectives on Merkle Tree Certificates, PLANTS and related approaches.

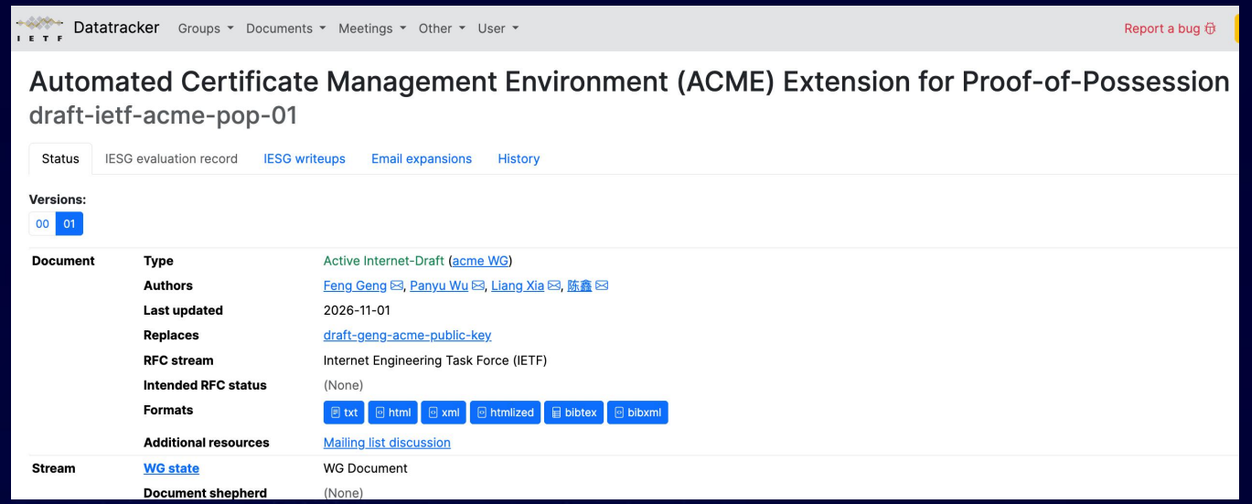
Participating affiliations include:

TrustAsia, Let's Encrypt, Keyfactor, Chainguard, Google/Chromium
(links go to the position papers)

12:40–13:40 — Lunch (on your own; see the venue notes above for options by Pankrác metro)

Datatracker Groups Documents Meetings Other User

Paper (S26): From End-to-End Test Deployment to Ecosystem Coordination: Lessons from Deploying Merkle Tree Certificates	Zoey Wang (TrustAsia Technologies). Position paper for the Monday 12 October 11:40 MTC/PLANTS roundtable. End-to-end MTC test deployment in the CQRP validation realm: ACME, Issuance Logs, Mirror cosigning, TLS credential selection, X.509 fallback, Chrome Canary validation; proposes a cross-component interoperability testing framework.
Paper (S49): ML-DSA Certificate issuance and the managed cloud gap	Zayn Lohiti (Chainguard). Position paper for the Monday 12 October 11:40 MTC/PLANTS roundtable. The software side of ML-DSA certificates works end to end; no public ...
Paper (S32): Report on the Implementation and Deployment of Merkle Tree Certificates for Post-Quantum Authentication	Aaron Gable, Josh Aas et al. (Let's Encrypt / Internet Security Research Group). Position paper for the Monday 12 October 11:40 MTC/PLANTS roundtable. Lessons from ...
Paper (S22): Post-quantum authentication for digital identity services in the cloud	Francis Lewis, Jess Wintertorne (UK Government Digital Service, Department for Science, Innovation and Technology). Position paper for the Sunday 11 October 09:30 slot in the ...
Slides 11_1130 Singh Zscaler: Beyond Algorithm Choice, lessons from preparing a large cloud proxy for PQ authentication	Slides for the Sunday 11 October 11:30 talk in the Performance and Embedded Systems session: Zscaler, Harpreet Singh and Yaroslav Rosomakho.
Slides 12_0830 Chairs: Welcome: Day 2 welcome, remote etiquette and agenda	Chairs welcome deck for Monday 12 October at Cisco: Day 1 recap, remote participation rules, format, Day 2 agenda with chairs, logistics, report timeline, closing ...
Slides 11_0900 Chairs: Welcome: Day 1 welcome, ground rules and agenda	Chairs welcome deck for Sunday 11 October at CTU: why we are here, Chatham House rule, code of conduct, format, Day 1 agenda with chairs, ...



Datatracker Groups Documents Meetings Other User Report a bug

Automated Certificate Management Environment (ACME) Extension for Proof-of-Possession
draft-ietf-acme-pop-01

Status | IESG evaluation record | IESG writeups | Email expansions | History

Versions: 00 01

Document	**Type**	Active Internet-Draft (acme WG)
	Authors	Feng Geng, Panyu Wu, Liang Xia, 陈鑫
	Last updated	2026-11-01
	Replaces	draft-geng-acme-public-key
	RFC stream	Internet Engineering Task Force (IETF)
	Intended RFC status	(None)
	Formats	txt html xml htmlized bibtex bibxml
	Additional resources	Mailing list discussion
Stream	**WG state**	WG Document
	Document shepherd	(None)

- TrustAsia took part in the IAB Workshop on Accelerating the Deployment of Post-Quantum Authentication
- TrustAsia published paper, *From End-to-End Test Deployment to Ecosystem Coordination: Lessons from Deploying Merkle Tree Certificates*

- TrustAsia contributed to IETF *draft-ietf-acme-pop-01*, which provides a protocol foundation for future support of post-quantum cryptographic algorithms, KEM keys, and other emerging key use cases.

亞洲誠信® TRUSTAsia

04

Preparing Your Organization for PQC

CBOM and Cryptographic Asset Discovery

Identify where cryptography is used and what depends on it:

Cryptographic assets

Algorithms, parameters, protocols, certificates, key metadata, libraries, and versions.



Upgrade constraints

Legacy clients, certificate pinning, manual updates, and product support lifecycles.

Business dependencies

TLS termination, applications, devices, CAs, CDNs, gateways, owners, and vendors.

亞洲誠信® TRUSTAsia

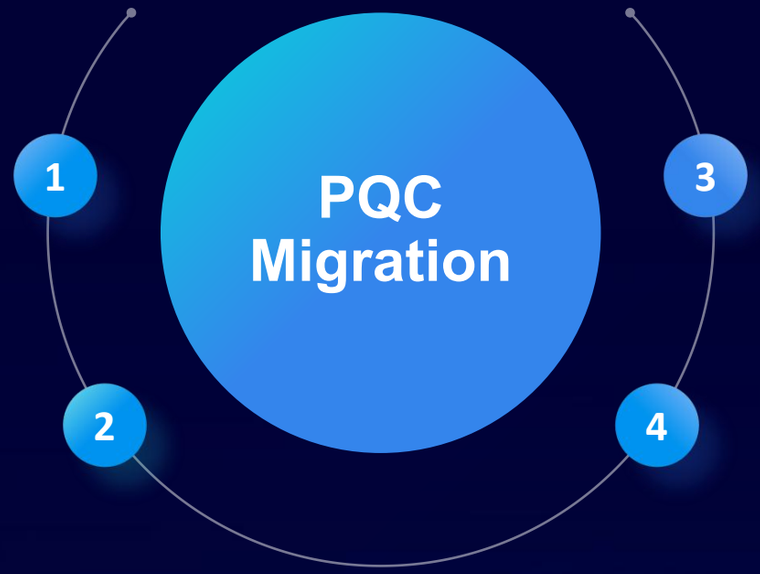
A PQC Migration Plan and Pilot Path

Discover assets

Build a CBOM and dependency map

Plan migration

Define paths, owners, and vendor dependencies



Prioritize risk

Protection lifetime, identity criticality, and upgrade cycles

Validate a pilot

Compatibility, performance, updates, and recovery

Plan separately

CA authentication, site authentication keys, and compatibility policy.

Automate early

Requests, renewal, deployment, reloads, and failure recovery.

Track support

CA, CDN, TLS software, device, and platform roadmaps.

亞洲誠信® TRUSTAsia

Building Repeatable Deployment Tests

Connect implementers and users through shared test scenarios

Cross-implementation testing

Connect more ACME clients, CAs, Mirrors, TLS stacks, and verifiers.

Failure scenarios

Test Mirror delays, expired Landmarks, version changes, and failed credential updates.

Automation and APIs

Improve asynchronous retrieval, multi-credential loading, renewal, and deployment.

Migration security

Validate compatibility paths together with client acceptance rules.

TrustAsia welcomes collaboration using our test services and deployment experience.

亞洲誠信® TRUSTAsia

MTCs provide the foundation
Migration connects old and new systems
Engineering collaboration enables adoption

Start with a cryptographic asset inventory, a pilot, and a set of interoperability tests.

亞洲誠信®
TRUSTAsia