

# 7<sup>th</sup> INTERNATIONAL CONFERENCE ON PUBLIC KEY INFRASTRUCTURE AND ITS APPLICATIONS (PKIA 2026)

SEPTEMBER 10-11<sup>th</sup>, 2026

## POST-QUANTUM TRANSITION FOR NATIONAL PKIs

HSMs, Long-Term Validation, and Lessons from Brazil and Latin America

JEAN EVERSON MARTINA · LabSEC / UFSC · BRAZIL



## The algorithms are ready. Are our trust infrastructures?

Standardization solved one layer. National trust infrastructures still have to move.

### ALGORITHMS

ML-KEM · ML-DSA · SLH-DSA

Standards are available. Implementations are maturing.

NIST



### TRUST INFRASTRUCTURE

HSM / keys

CA / RA / SGC

certificates

signatures

timestamps

validators

preservation

cross-border  
trust

The difficult part is migrating the system around the algorithms.

## Two theses for this talk

1

The post-quantum transition is a trust-infrastructure migration problem.

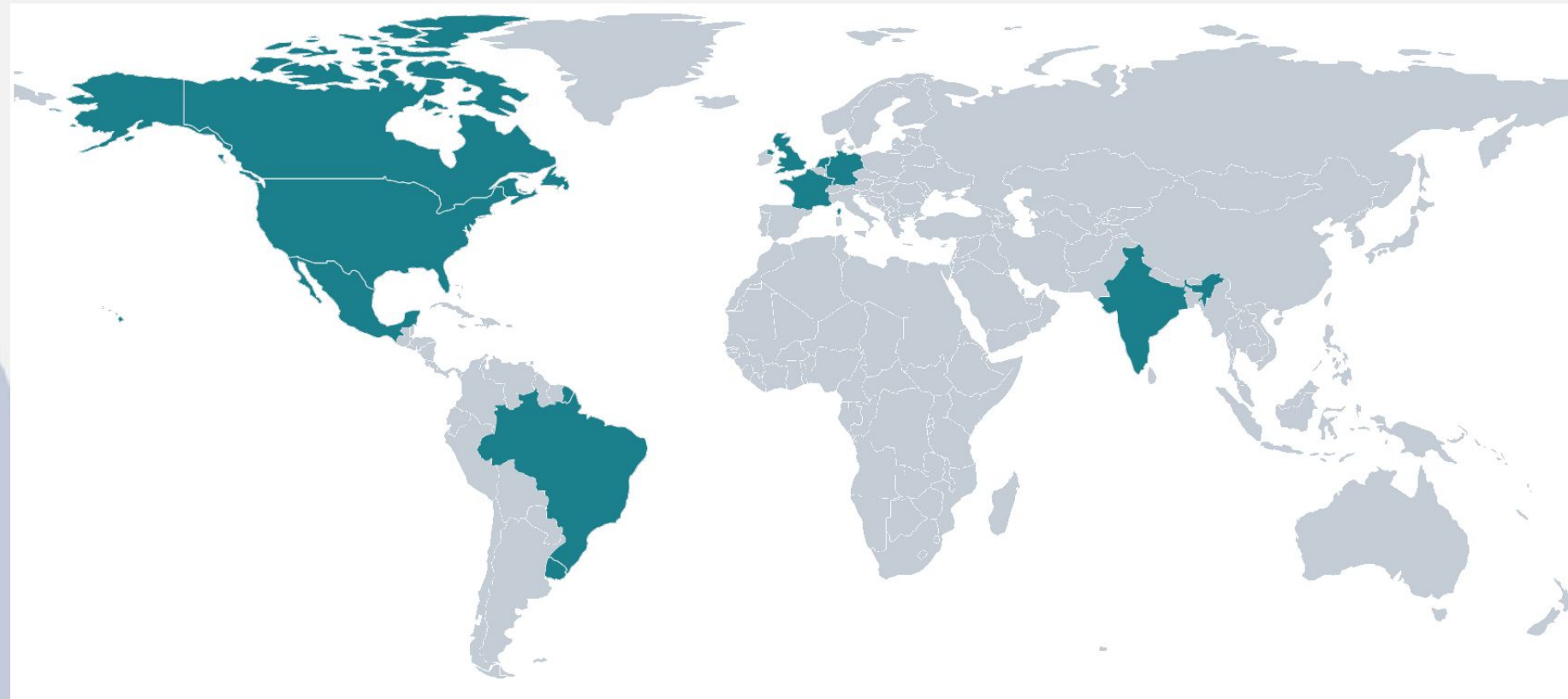
2

Without coordination, Latin America risks creating post-quantum trust islands.

These are different problems — and PKI sits at the intersection of both.

## The global transition has already started

Different jurisdictions are converging on staged migration, inventory, crypto-agility and deadlines.



### NIST

FIPS 203 / 204 / 205

2024

### EU

transition starts

2026

### INDIA

CII resilient

2029

### US

HVA key  
establishment

2030

### UK / CANADA

priority systems

2031

### UK / CANADA

full migration

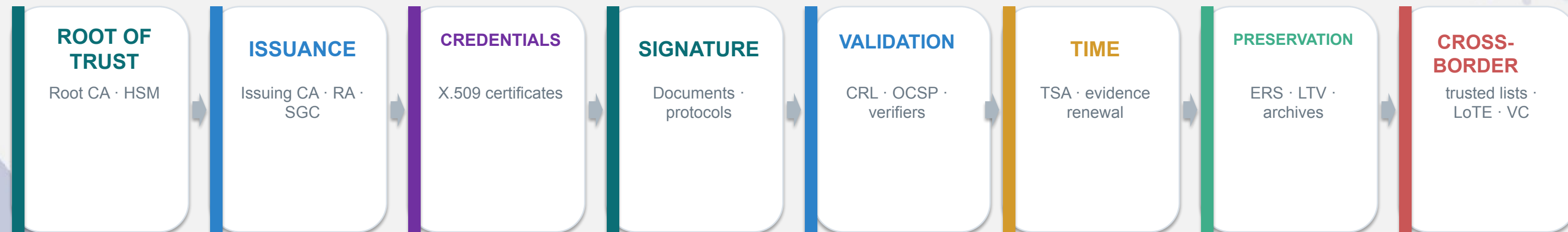
2035

**Netherlands / TNO: practical migration methodology rather than another algorithm catalogue.**

Public roadmaps and policies: NIST · European Commission · NCSC UK · Cyber Centre Canada · DST India · AIVD/CWI/TNO.

## What actually has to migrate?

PQC migration is a dependency graph, not a switch.



A system can be “post-quantum” in one layer and still depend on classical cryptography elsewhere.

Our gov.br experiment exposed exactly that dependency problem.

## Latin America: one region, very different starting points

Classification reflects the type of public evidence found — not a maturity ranking.



### **Normative / implementation**

Brazil · Ecuador

### **Policy / roadmap**

Uruguay · Peru · Chile · Colombia

### **Research / pilot**

Mexico · Costa Rica–Uruguay

### **Readiness / political R&D**

Argentina · Guatemala · Panama · Dominican Rep. · Cuba

### **Baseline PKI / no public PQC instrument located**

Paraguay · Bolivia · El Salvador · Honduras · Haiti · Nicaragua

### **Evidence gap**

Venezuela

**“Not located publicly” ≠ “does not exist”.**

## Three transition paths

The region is not moving in one sequence.

### BRAZIL

Normative enablement, domestic HSM support and end-to-end experimentation.

**REGULATION + ENGINEERING**

→ deployment

### URUGUAY

National strategy explicitly calls for a quantum-resistant national PKI.

**POLICY MANDATE**

→ architecture

### MEXICO

A concrete PQ-PKI project creates a technical path that can feed government adoption.

**RESEARCH + ENGINEERING**

→ public uptake

**Different starting points demand a common migration methodology — not a single technical recipe.**

## Brazil: beyond algorithm selection

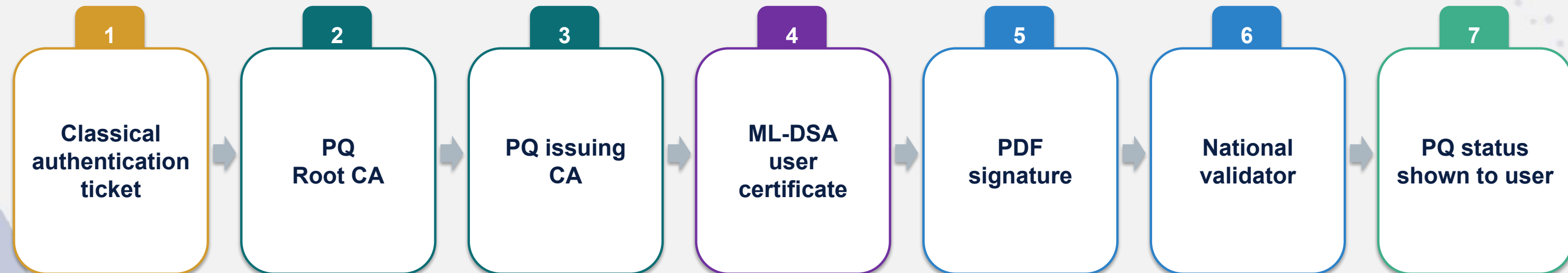
A national PKI stack that is increasingly implementation-ready — with a conformity and deployment gap.

|                             |                                                                      |                    |
|-----------------------------|----------------------------------------------------------------------|--------------------|
| <b>Normative framework</b>  | ML-DSA / ML-KEM included in DOC-ICP-01.01 v6.0                       | READY              |
| <b>HSM ecosystem</b>        | Dinamo + Kryptus commercial support for NIST PQC algorithms          | READY              |
| <b>CA software</b>          | ITI–UFSC SGC can issue classical, PQ and hybrid profiles             | WORKING            |
| <b>End-to-end signature</b> | PQ root → user cert → PDF → national validator                       | DEMONSTRATED       |
| <b>Timestamp capability</b> | Hardware capability reported by timestamp providers                  | TECHNICALLY VIABLE |
| <b>MCT / homologation</b>   | Conformity manuals, certification profiles and deployment procedures | GAP                |

Brazil is no longer waiting for algorithm selection; the bottleneck has shifted to conformity and operational deployment.

## An end-to-end PQ signature experiment in gov.br

Pure ML-DSA — from a new PQ root to the national validator.



**The signature path was post-quantum. The identity-proofing ticket that triggered issuance was still classical.**  
That is the migration problem in one diagram.

## What the Brazilian experiment taught us

A migration can succeed technically and still be incomplete systemically.

### DEMONSTRATED

- PQ root and issuing CA
- Pure ML-DSA end-user certificate
- PDF signing
- National signature validation
- Explicit PQ status to the user

### STILL TO MIGRATE

- Authentication mechanism
- Conformity / MCT procedures
- Production certification profiles
- Operational rollout
- Remaining dependent services

Migration readiness must be assessed by dependencies, not by a single “PQC supported” checkbox.

## Uruguay: policy before architecture

A strong national objective — with the implementation profile still open.

### NATIONAL CYBERSECURITY STRATEGY 2024–2030

Develop a new national public-key infrastructure resistant to the threats of quantum technology, aligned with international standards and adopting post-quantum algorithms.

#### Publicly defined

policy mandate

#### Not publicly defined yet

algorithm profile

HSM / token profile

migration sequence

hybrid / pure policy

conformity path

Uruguay shows the opposite sequence from Brazil: the policy objective is explicit before the engineering profile is fixed.

Source: Uruguay National Cybersecurity Strategy 2024–2030 (AGESIC).

## Mexico: engineering before national policy

A research-led path with a concrete PQ-PKI project.

### IPN · CIC · 2026

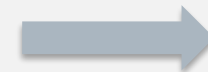
Development of a post-quantum Public Key Infrastructure (PKI) for applications at IPN



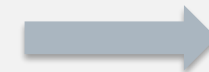
### POTENTIAL POLICY UPTAKE

Technical testbeds can reduce uncertainty before a government commits to a national migration profile.

RESEARCH



ENGINEERING



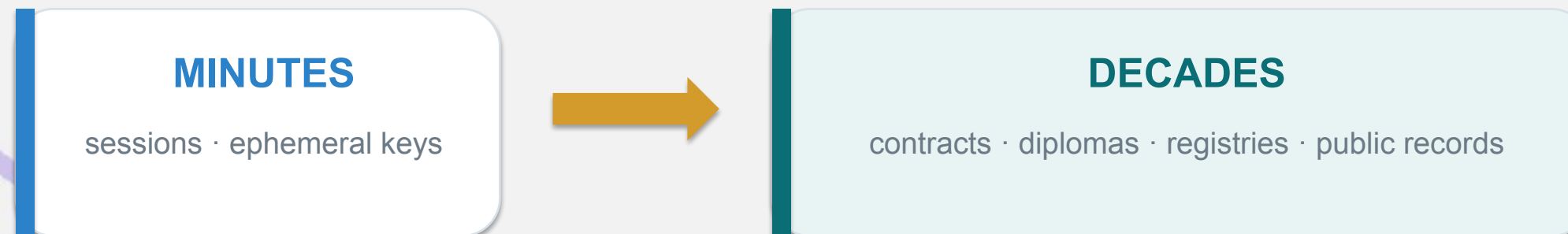
PUBLIC UPTAKE

**Mexico illustrates a third path: engineering can lead — and later shape policy.**

Public source: CIC-IPN research project listing, 2026.

## The harder problem: decades, not sessions

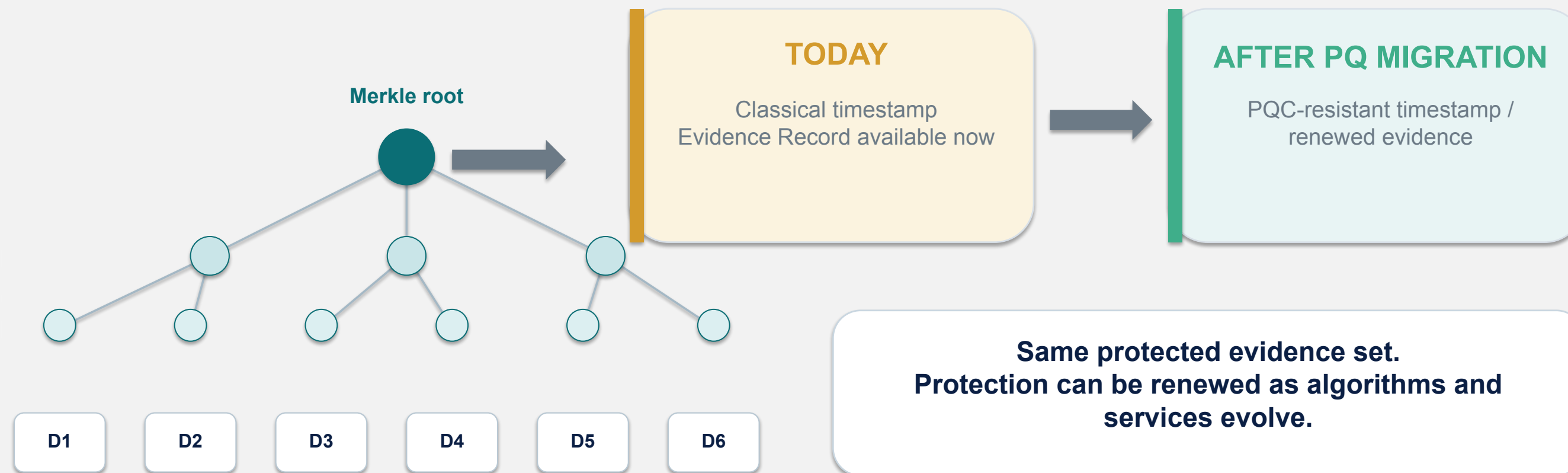
TLS connections expire in minutes. Public records may need to remain trustworthy for decades.



The transition must preserve evidentiary value — not just future cryptographic strength.

## Preserving trust across the quantum transition

Use evidence renewal to carry integrity across algorithm generations — without rewriting history.

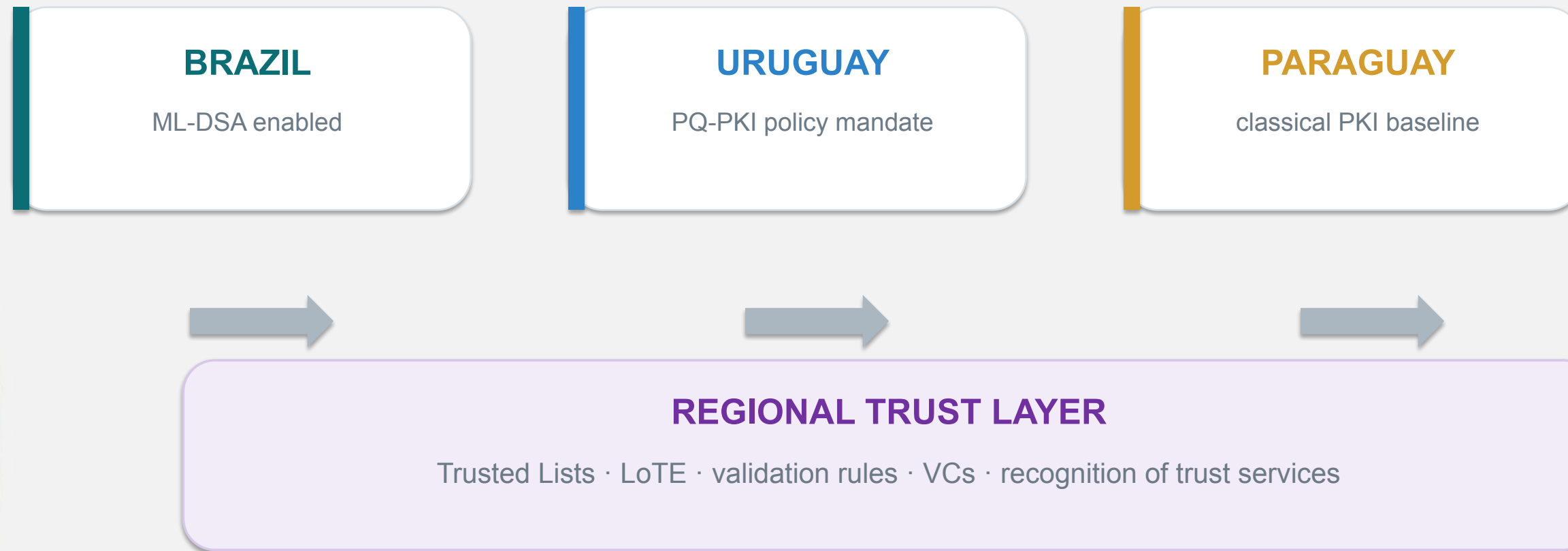


**Protect what already exists — not only what we sign after migration.**

Conceptual strategy based on Evidence Record Syntax (RFC 4998) and ongoing ETSI ESI work on PQC impact in preservation services.

## Nationally secure does not mean regionally interoperable

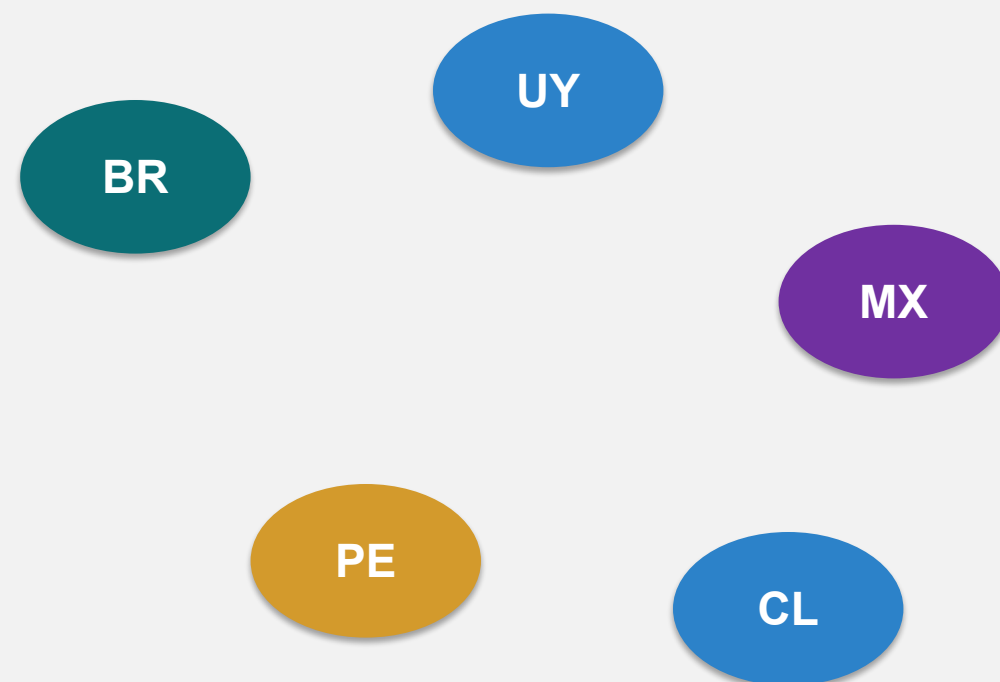
Cross-border trust turns PQC into a coordination problem.



If national migration profiles diverge, cross-border validation can fail even when every country is “secure” on its own.

## Do not replace classical trust islands with post-quantum trust islands

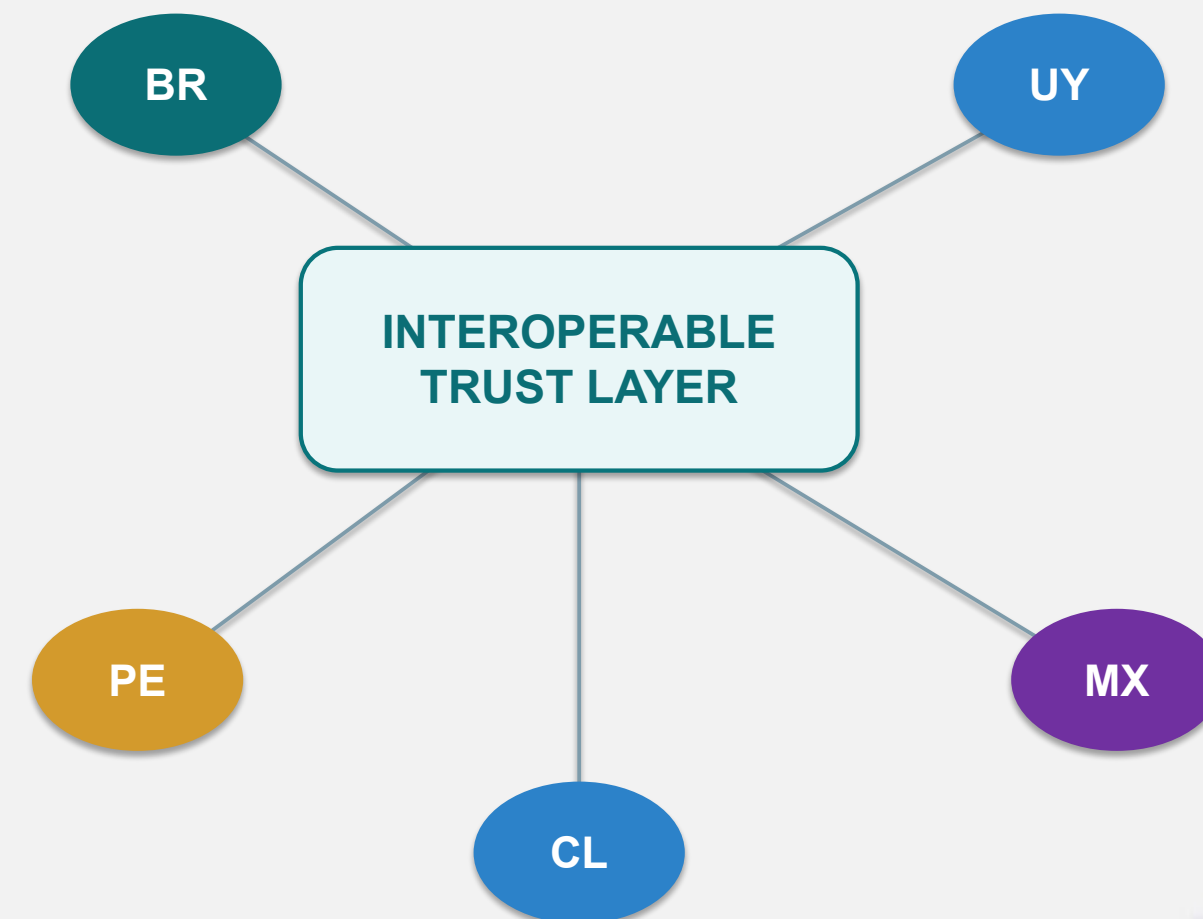
WITHOUT COORDINATION



different algorithms · profiles · timelines



WITH A REGIONAL MIGRATION PROFILE

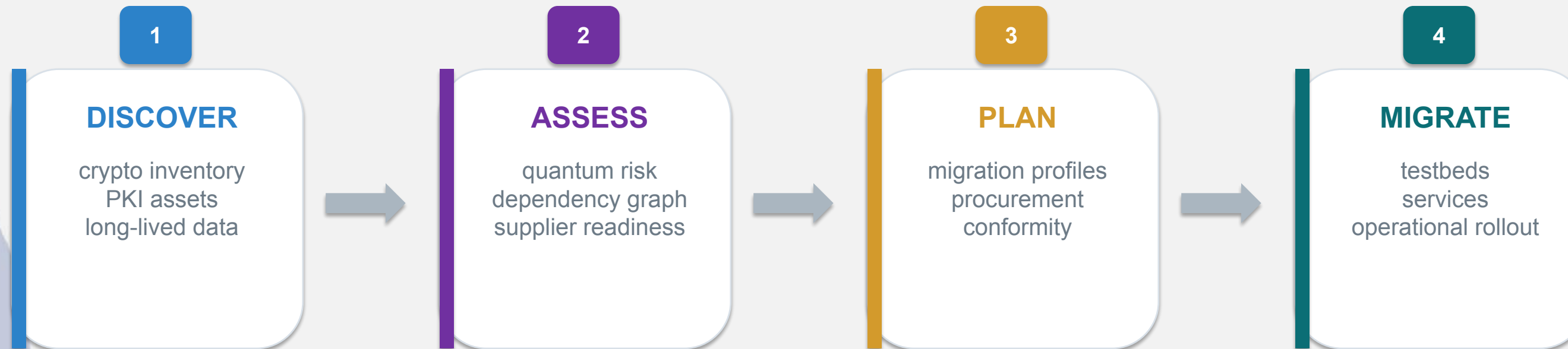


shared migration principles · validation expectations ·  
crypto-agility

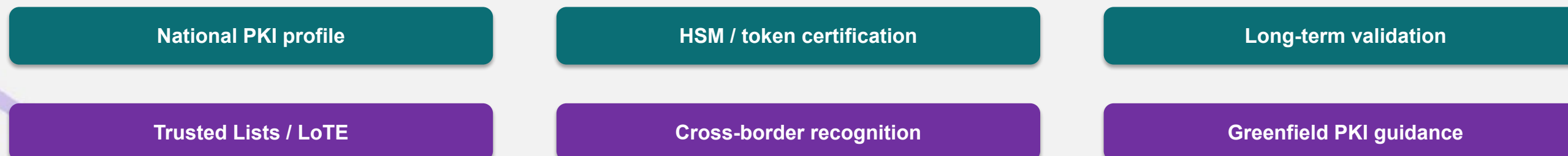
Coordination is a security property of cross-border trust.

## What Latin America needs: a migration methodology

Start from the Dutch handbook — extend it for national PKIs and cross-border trust.



### LATAM EXTENSIONS



The goal is not to copy the Dutch handbook — it is to make it work for a multi-jurisdiction trust ecosystem.

## From national experiments to a regional approach

### UFSC + IPN are starting to structure an initiative towards a Latin American PQC transition guide

building on national PKI experience, research testbeds and international migration methodologies

#### INVENTORY NOW

Know where public-key cryptography and long-lived trust actually live.

#### BUILD CRYPTO-AGILITY

Into PKIs, HSM procurement, validators and trust services — not only applications.

#### COORDINATE EARLY

Before national solutions diverge and interoperability becomes the next migration.

**The next challenge is not choosing a post-quantum algorithm.  
It is migrating trust without breaking it.**

# THANK YOU

Questions?

Jean Everson Martina · LabSEC / UFSC

jean.martina@ufsc.br



## APPENDIX

Sources, evidence matrix and Brazil technical readiness.

### Backup material for discussion and Q&A

LATAM EVIDENCE

BRAZIL READINESS

PUBLIC SOURCES

## Appendix · LATAM evidence matrix

Public evidence located as of 9 Sep 2026.

| Country            | Evidence type              | Public signal                                                         | Class |
|--------------------|----------------------------|-----------------------------------------------------------------------|-------|
| Brazil             | Normative + implementation | ML-DSA/ML-KEM in ICP-Brasil; commercial HSMs; end-to-end test         | A/C   |
| Uruguay            | Policy mandate             | National strategy explicitly calls for quantum-resistant national PKI | A     |
| Peru               | Roadmap                    | Quantum-safe planning for banks, identity and public registries       | B     |
| Chile              | National quantum strategy  | PQC + pilots in 2025–2035 strategy                                    | B     |
| Colombia           | Digital-security strategy  | National capabilities in quantum computing and PQC                    | B     |
| Mexico             | Research / pilot           | Explicit PQ-PKI project at IPN                                        | C     |
| Costa Rica–Uruguay | Trust-service project      | Quantum-resistant long-term archive / trust service                   | C     |
| Argentina          | Legislative / R&D          | Bill proposes mandatory APN PQC migration in 5 years                  | D     |
| Guatemala          | Readiness discussion       | Inventory, procurement and roadmap recommendations                    | D     |

Additional directed searches: Paraguay · Bolivia · El Salvador · Honduras · Haiti · Nicaragua · Dominican Republic · Cuba · Panama · Venezuela.

## Appendix · Brazil technical readiness

What exists today, what was demonstrated, and what remains.

|                     |                                                                 |                      |
|---------------------|-----------------------------------------------------------------|----------------------|
| DOC-ICP-01.01 v6.0  | ML-DSA / ML-KEM included                                        | PUBLIC / NORMATIVE   |
| Dinamo + Kryptus    | NIST PQC algorithms in commercial HSM portfolios                | PUBLIC / PRODUCT     |
| ITI-UFSC SGC        | Classical, PQ and hybrid-capable issuance paths                 | PROTOTYPE            |
| gov.br experiment   | Pure ML-DSA root, issuance, PDF signing and national validation | DEMONSTRATED         |
| Timestamp providers | PQC-capable equipment reported                                  | TECHNICAL CAPABILITY |
| MCT / homologation  | Detailed conformity and deployment profiles                     | OPEN GAP             |

Working description: deployment-ready stack with a conformity gap — not a nationwide operational migration yet.

## Appendix · Key public references

|                  |                                                                    |
|------------------|--------------------------------------------------------------------|
| NIST             | FIPS 203/204/205 and Post-Quantum Cryptography project             |
| Brazil · ITI     | DOC-ICP-01.01 v6.0; IN 35/2026; GTT-PQC/ICP-Brasil                 |
| Uruguay · AGESIC | National Cybersecurity Strategy 2024–2030                          |
| Mexico · IPN     | CIC research project: post-quantum PKI for IPN applications        |
| Netherlands      | AIVD · CWI · TNO — PQC Migration Handbook                          |
| EU               | European Commission coordinated PQC roadmap; ETSI ESI PQC work     |
| UK / Canada      | NCSC migration timelines; Government of Canada PQC roadmap         |
| India            | DST Quantum-Safe Ecosystem in India; MeitY PQ-PKI engineering work |
| Evidence Records | RFC 4998 — Evidence Record Syntax (ERS)                            |

Full URLs and document identifiers can be moved into presenter notes in the next revision.