ASIA DIGITAL TRUST SUMMIT 2026 · COLOMBO

TRUST IN LATIN AMERICA THE PQC TRANSITION

Regional migration paths and interoperability challenges

Jean Everson Martina · LabSEC · UFSC, Brazil

UNIVERSIDADE FEDERAL DE SANTA CATARINA

LATIN AMERICAN DIGITAL TRUST

National trust systems face a shared transition

TODAY

National PKIs protect public services and records

NEXT

PQC changes keys, systems, policies and validation

Choices made nationally will shape regional interoperability.

THREE PQC MIGRATION PATHS

Different paths, shared challenge

BRAZIL

ICP-Brasil PQC rules
HSM and CA engineering
ML-DSA signing test

URUGUAY

National PQ-PKI objective
Profiles still emerging
Policy-led migration

MEXICO

CIC-IPN PQ-PKI project
Research and prototypes
Pilot opportunities

Different sequences will eventually meet at the same border.

PQC migrates the whole trust chain

ALGORITHMS

Keys and certificates
Signature profiles

INFRASTRUCTURE

HSM and CA systems
Validator software

GOVERNANCE

Policies and conformity
Historical evidence

Migration has to cover the chain behind each signature.

ITI–UFSC EXPERIMENT · BRAZIL

Brazil: a post-quantum signing test

NOW

PQ root and user certificate
ML-DSA PDF and national validation

NEXT

Authentication, conformity
production and foreign validation

A pure ML-DSA test demonstrated technical feasibility, not national rollout.

LONG-TERM DIGITAL TRUST

Public documents outlive today's algorithms



Classical archives; PQC pilots

Migration profiles; algorithm retirement

Historical trust needs renewable evidence

Evidence must be renewed before algorithms lose trust.

CROSS-BORDER TRUST

Cross-border trust needs historical evidence

SIGNING POLICY

What was acceptable when it was signed?

SERVICE STATUS

Which service was trusted?
When did it change?

FOREIGN VERIFIER

Can another country reconstruct that decision?

Trusted Lists aid verification; legal recognition is national.

REGIONAL INTEROPERABILITY

Independent verifiers can disagree

1

Parse signature

ML-DSA support
Document profile

2

Build trust

Foreign trust root
Service policy

3

Check evidence

Revocation, time
Renewal history

4

Explain result

Valid / invalid
or indeterminate

Interoperability requires comparable conclusions and clear reasons.

A REGIONAL PQC MIGRATION AGENDA

Shared tests before profiles diverge

INVENTORY

Roots, HSMs, CAs and hidden dependencies

PROFILES

Algorithm choices
Certificate formats

EVIDENCE

LTV, timestamps and evidence renewal

VALIDATION

Trusted Lists
Foreign trust decisions

The objective is common test criteria, not one regional PKI.

AN INVITATION TO APKIC MEMBERS

Let's test cross-border post-quantum trust

Asia–LATAM pilot: signed samples, independent validation and a gap report in 60 days.

Jean Everson Martina · LabSEC / UFSC, Brazil
jean.martina@ufsc.br

UNIVERSIDADE FEDERAL
DE SANTA CATARINA