CHELPIS
Chelpis Quantum Corp.

2025 Post-Quantum Cryptography Forum @ MITRE, 20251027

# Taiwan's PQC Migration Framework: Securing the Global Semiconductor Supply Chain

Ming Chih
Founder & CEO

CHELPIS
Chelpis Quantum Corp.

CHELPIS

Founded @ 2017

# Ming Chih

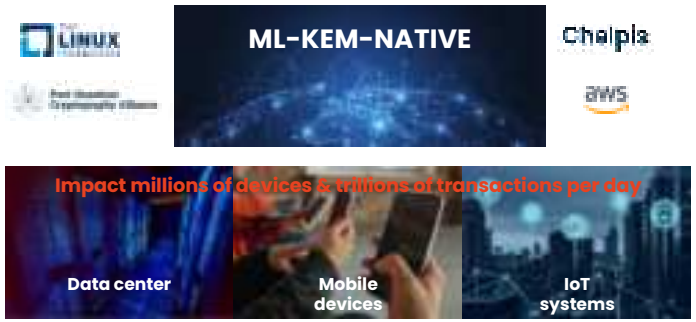
| | |
|---|---|
| CHELPIS QUANTUM COPR. | CEO |
| Taiwan Quantum Safe Migration Center | CEO |
| Taiwan Drone Technology Associate | Director |
| RISC-V Taiwan | Director |


**CHELPIS Public project**

2017 ~ NIST PQC Additional Digital Signature
2024~ Taiwan Quantum Safe Migration
2024~ Linux Foundation PQC Alliance PQC Open Source
2025~ Taiwan Drone Resue Initiative

CHELPIS

Founded @ 2017




**LibOQS**

**The largest Quantum-Safe open source library**

## PQC Research

Chelpis QSMC

### NIST Selected 2nd

UOV

MAYO

### Organization

MITRE PQC Coalition

THE LINUX FOUNDATION

NIST

### Publication

- **KyberSlash:** Exploiting secret-dependent division timings in Kyber implementations
- **Nibbling MAYO:** Optimized Implementations for AVX2 and Cortex-M4
- **Fast and Clean:** Auditable high-performance assembly via constraint solving

### Open Source Software

- Mlkem-c-aarch64
- Mlkem-c-embedded
- MAYO in Go
- FrodoKEM Jasmin

# Taiwan PQC Ecosystem

## Promote the PQC market by establishing a collaborative ecosystem among industry, government, and research

**Hosted 20+ workshop & events with 80+ experts globally.**

NIST National Institute of Standards and Technology
MITRE
THE LINUX FOUNDATION


**Initiated PQC alliances and formed partnerships with 30+ partners.**

TAIWAN QUANTUM SAFE Association 臺灣量子安全產業協會
QSMC
DoQubiz
Openfind
SHIELD XTREME

**Facilitated government programs and fostered 25+ PQC products this year.**

moda 數位發展部 Ministry of Digital Affairs
數位產業署
ITRI Industrial Technology Research Institute
財團法人資訊工業策進會 INSTITUTE FOR INFORMATION INDUSTRY

# Taiwan PQC Ecosystem

**Promote the PQC market by establishing a collaborative ecosystem among industry, government, and research**

Taiwan needs early quantum-safe migration to stay in the game

Taiwan advised to attract post-quantum cryptography talent, make migration cost as low as possible TAIPEI (Taiwan News) — With more...

Progress in quantum computing poses potential security risk in Taiwan

Experts urge governments to migrate to post-quantum cryptography to protect vital assets, privacy 2023/10/16 11:19 By Sean Scanlan...

Taiwan needs coordinated approach to create robust cybersecurity

Taiwan should maximize strengths, focus on areas that have potential to be developed into niche markets

# Taiwan Migration framework

## Government

2023 PQC be National Critical Technology
2024 PQC industry promotion for 5 years
2025 Ministry of Digital Affair -> Migration Guildeline 1.0,
2026 Financial Supervisory Commission -> FS Guideline
2027 PQC Roadmap

# Taiwan Migration framework

## Government

moda 數位發展部 Ministry of Digital Affairs

Taiwan is emerging as a global hub for post-quantum cryptography (PQC) development. It regularly hosts world-renowned academic conferences such as ACM conference, Asia crypt, CHES (Cryptographic Hardware and Embedded Systems), and Real World Crypto (RWC). The team led by Dr. Bo-Yin Yang at Academia Sinica plays an active role in the **NIST PQC competition**, contributing significantly to algorithm design and cryptanalysis.

With this strong foundation, Taiwan has nurtured a deep bench of cryptographic experts. Combined with the nation's semiconductor strengths and strong government support for cybersecurity, Taiwan has built a globally competitive PQC innovation ecosystem. Post-quantum cryptography has been officially designated as a National Key Technology, overseen by the Ministry of Digital Affairs (MoDA). Additionally, in its newly released National Cybersecurity Strategy 2025, Taiwan has explicitly identified quantum security as a national defense priority—advancing the principle that "**Cybersecurity is National Security**."

Since 2023, MoDA has actively launched PQC policy initiatives, including the development of **Open chip design platforms** and reference development kits supporting algorithms such as ML-KEM (FIPS 203) and ML-DSA (FIPS 204). These efforts enable Taiwan's chipmakers to rapidly align with global standards and accelerate the creation of a trusted, quantum-resilient semiconductor infrastructure.

CHELPIS
Chelpis Quantum Corp.

# Taiwan Migration framework

## Government

PQC Industry Promotion 2024 - 2029

Identity


Digital Sig

PQC IP


FPGA

CHELPIS
Chelpis Quantum Corp.

# PQC Migration Guideline

## Government

**Announced at 2025/4/16**

Key Takeaway :
Taiwan follow US standard and refer EU's guildeline.
Build the Guideline


PQC-CIA
PQC Cybersecurity Industry Alliance

**Reference :**

NIST-SP-1800-38A、

NIST-SP-1800-38B、

NIST IR 8547 、

QUANTUM-READINESS ： MIGRATION TO POSTQUANTUM

TNO CWI AIVD The PQC Migration Handbook


CHELPIS
Chelpis Quantum Corp.

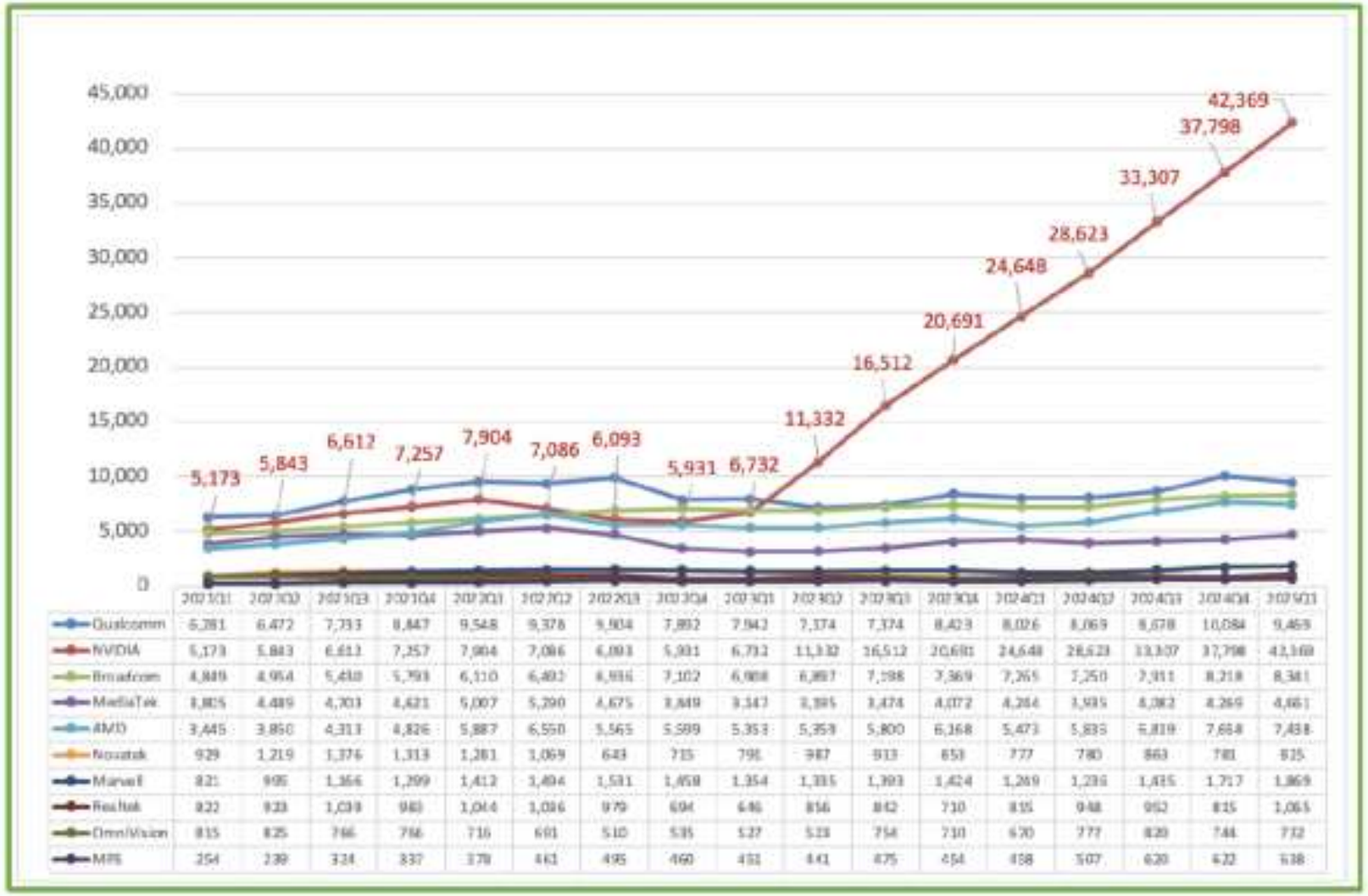
# Taiwan Migration framework

## Industry

- Semiconductor ecosystem
    - Drive by supply chain
- PQC StartUp company with government fund
    - Chip innovation fund for 10 years.
- PQC products
    - Network
    - Certificate
    - New application build with PQC
- PQC Tesing lab update

CHELPIS
Chelpis Quantum Corp.

# Global Top Ten Fabless IC Design Companies by Revenue: 2021-2025 Q1




Taiwan Chip Company Will finished PQC on New product design by **2027**

CHELPIS
Chelpis Quantum Corp.

# PQC Semiconductor ecosystem in Taiwan

**Chip Innovation USD 1.6 B**
**100M+ PQC project**

**30+ VENDER WITH PQC**
**70% market share on TV/ NB**

**70% market share**
**PQC Silicon IP ready**

## Policy Research

中央研究院 ACADEMIA SINICA

ITRI Industrial Technology Research Institute

III

moda 數位發展部 Ministry of Digital Affairs

## Industry Chip Design

MEDIATEK

REALTEK

NOVATEK

acer

ASUS

WNC Wistron NeWeb Corp.

ZYXEL NETWORKS

CHELPIS

GUC

JMEM TEK

Wisecure technologies 慧安安全

PUFsecurity 熵码科技

## Foundries

tsmc

UMC

ememory

GlobalFoundries

QSMC

CHELPIS Chelpis Quantum Corp.

# PQC ready chip design ongoing



**Industy fund**
**Government fund**
**Supply chain needed**








# PQC product for Network

**Unidirectional gateway**

**PQC ready Encryption**

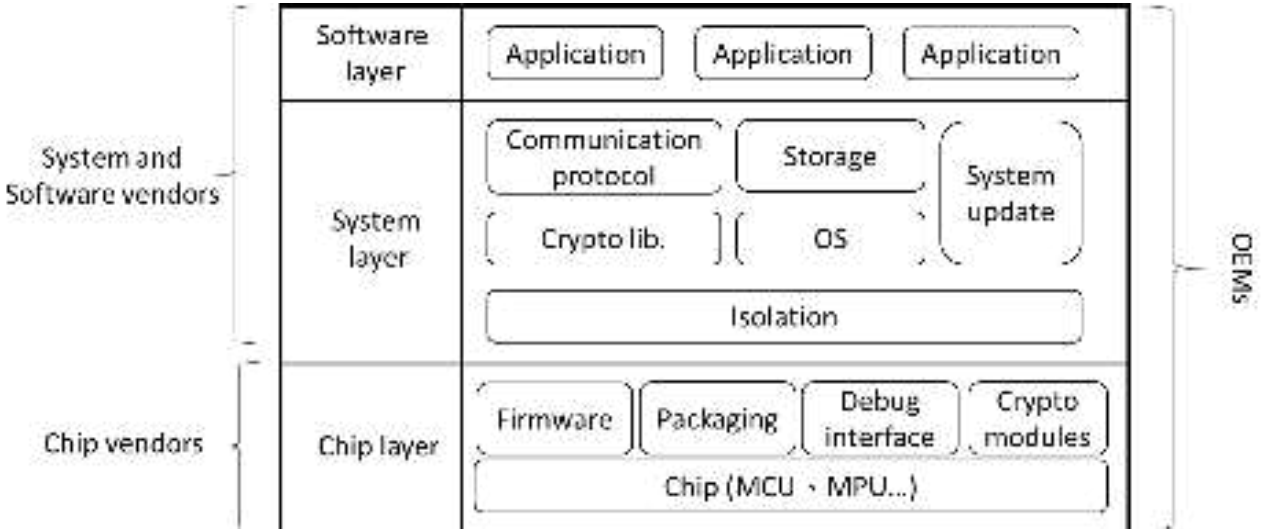
Support NIST ML-KEM and ML-DSA Level 1, 3, 5

CHELPIS
Chelpis Quantum Corp.

# PQC on RF & DRONE APPLICATION

# Taiwan Chip Security Standards published as Industry Standard since Nov. 2022

- ICT products can usually be divided into the most basic chip layer, as well as the system layer and software layer that builds them. Different vendors are responsible for developing the relevant software and hardware components.
- The scope of application of this series of standards is various software and hardware components that constitute ICT products, and these components will bring potential security risks to the products.



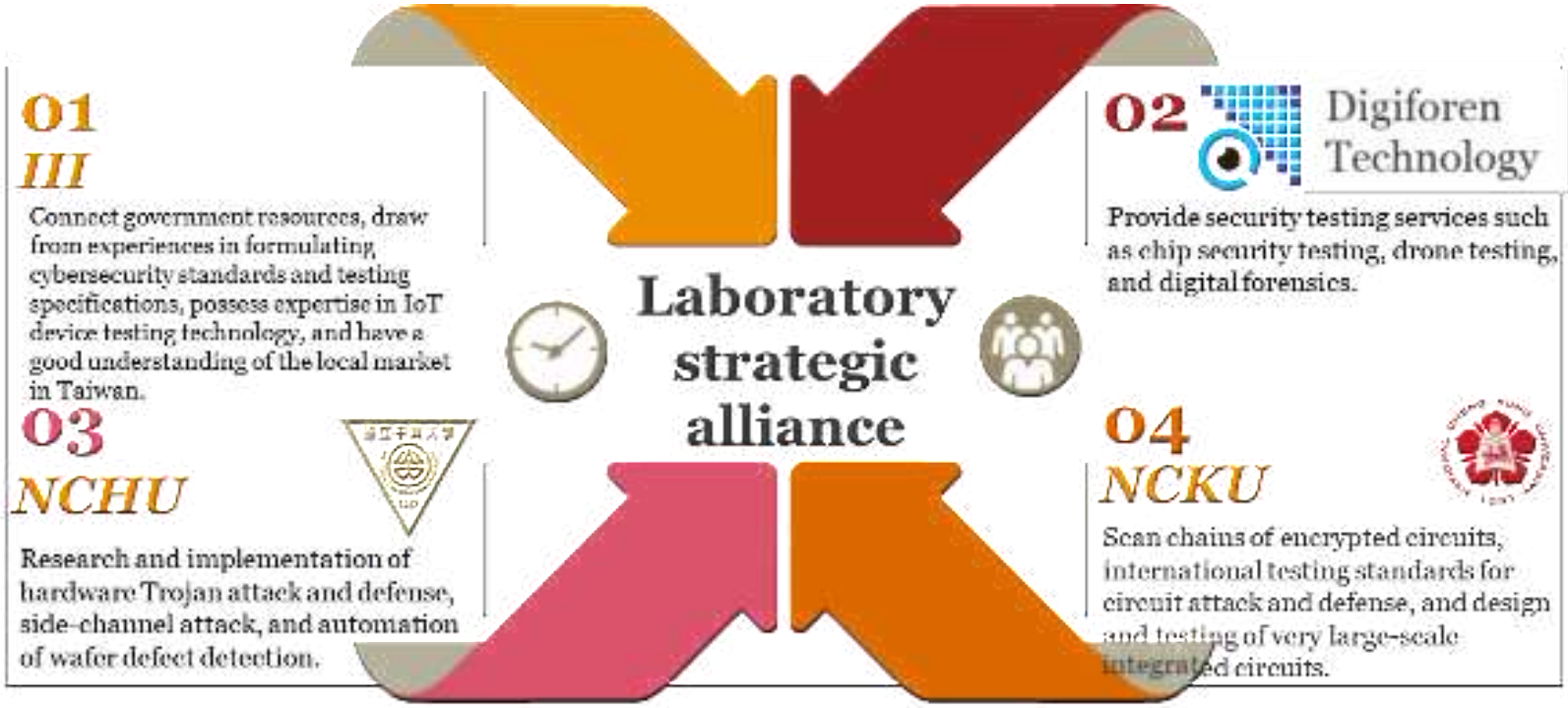

30+ organizations

CHELPIS
Chelpis Quantum Corp.

# Laboratory Strategic Alliance

- **Based on the approach of a strategic alliance, all parties collaboratively build capacity through human resources (domain experts), material resources (testing equipment), facilities (labs), and business transfer models.**

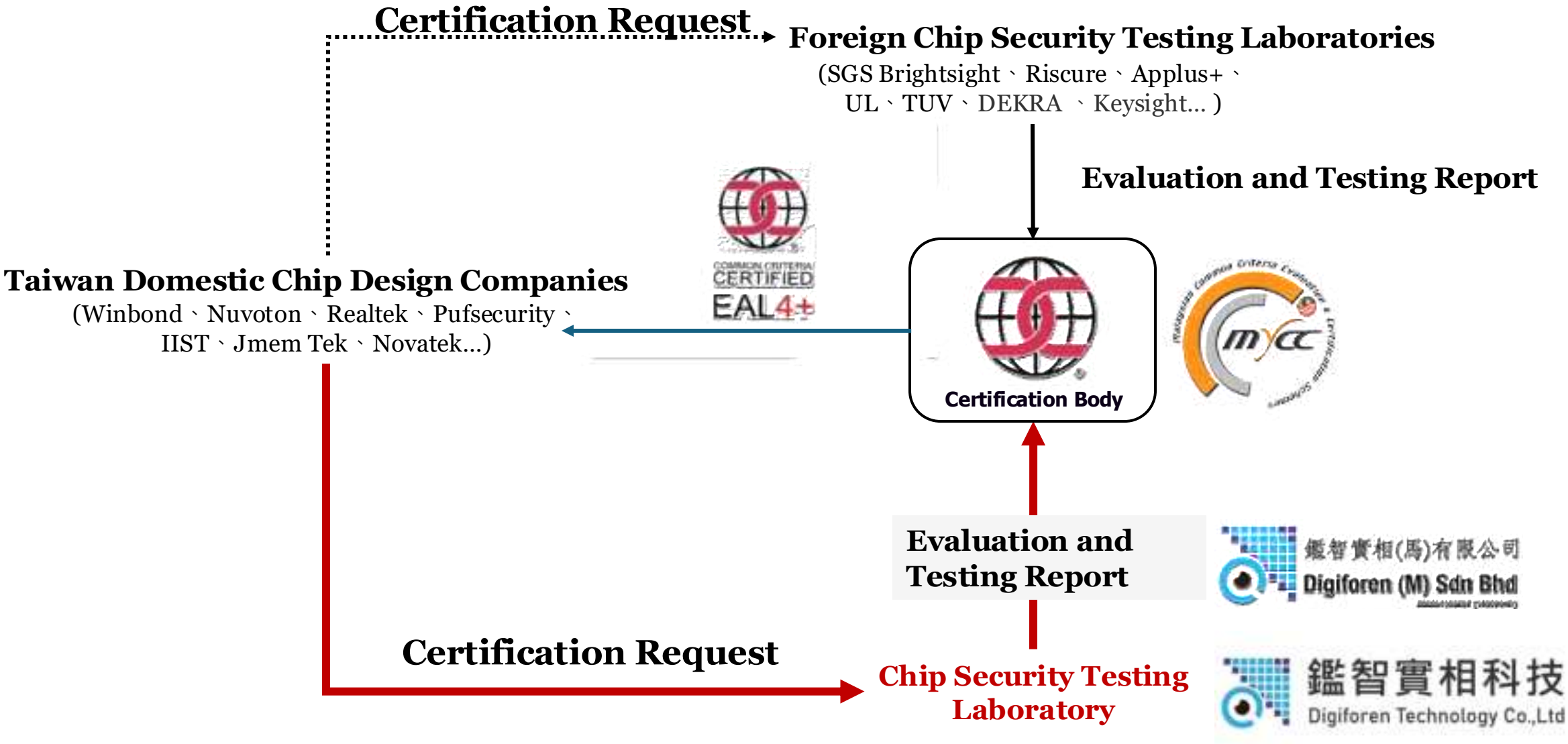
1. *Focus on SESIP & PSA*
2. *Equipped with SCA & FI (Riscure B.V.)*




1. *Focus on Common Criteria*
2. *Equipped with SCA, FI & Laser (Riscure B.V. & Secure-IC)*

CHELPIS
Chelpis Quantum Corp.

# CC Chip Certification Model




CHELPIS

# Summary & ongoing priority

## Industry

- Semiconductor supply chain is now being driven by regulatory frameworks such as the EU Cyber Resilience Act (CRA) and the US Commercial National Security Algorithm Suite (CNSA 2.0).
- Across industries, leading companies are aligning toward a common goal: to become “PQC-ready” between 2026 and 2028—meeting global compliance requirements and protecting critical infrastructure.
- To support this transition, independent testing labs are being established to issue PQC compliance and performance testing, enabling validation of algorithms, hardware integration, and side-channel resistance.

CHELPIS
Chelpis Quantum Corp.

# Summary & ongoing priority

## Government

1. Finical agency **set**

   **the Certificate infrastructure** in priority.

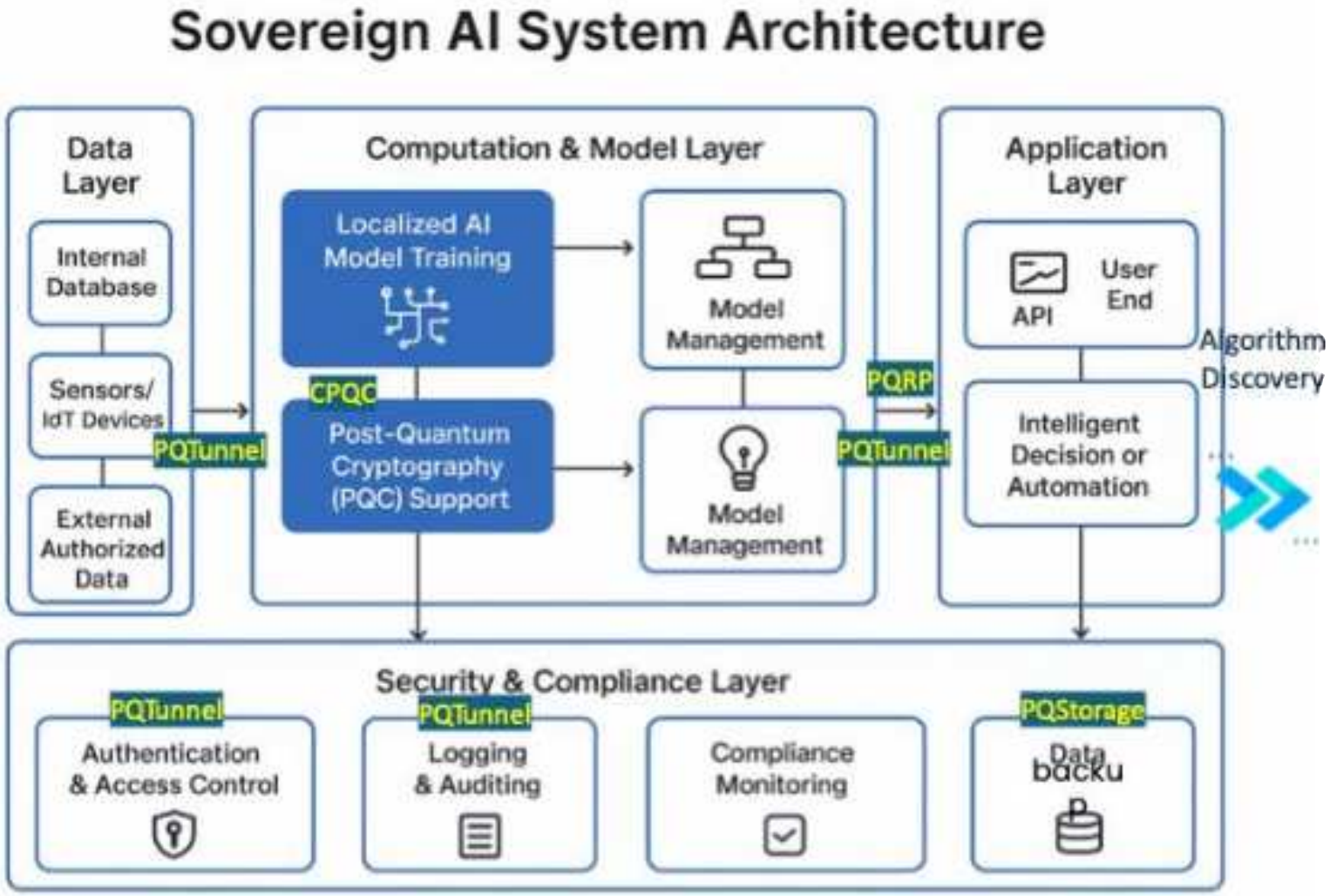
2. PQC guideline >> PQC Roadmap

3. Chip innovation fund fully support PQC.

CHELPIS
Chelpis Quantum Corp.


WELLCOME TO TAIWAN
RWC @ Taipei
March 9–11, 2026
CHELPIS

# PQC AI Data Center interoperability




PQScan