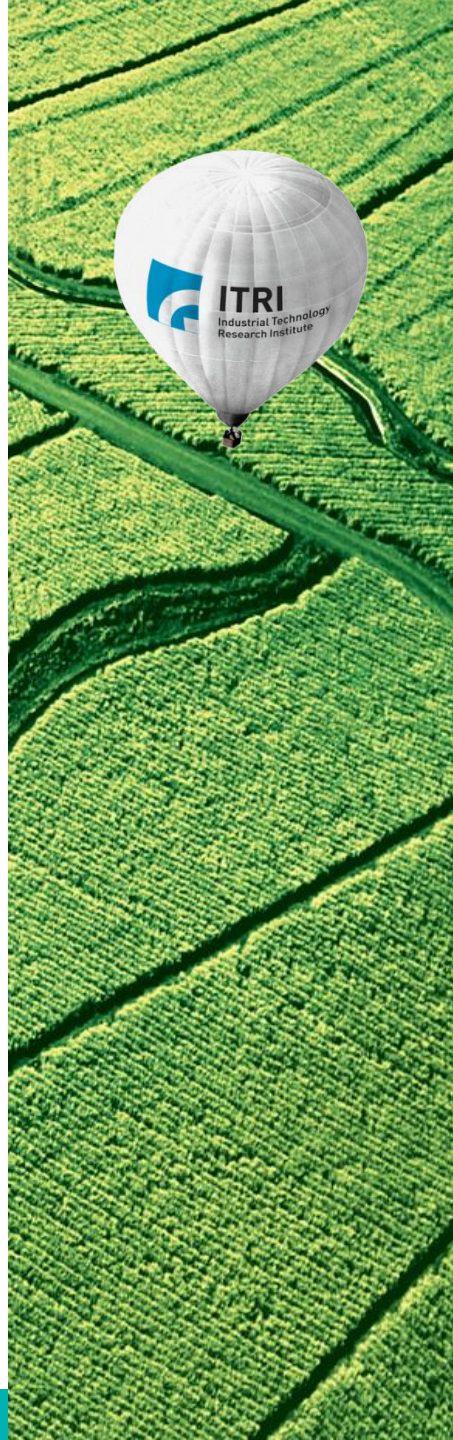
ITRI
Industrial Technology
Research Institute



PQC-Enabled Security Dongle: Hybrid FIDO2 & X.509 Certificate Solution

Mr. Derek Chen, Technical Manager
Industrial Technology Research Institute (ITRI)
E-mail: derekchen@itri.org.tw

2025/8/5

About ITRI (Industrial Technology Research Institute)

"Innovate for industry. Create value for society."

Who We Are

- Founded in **1973**, under **Taiwan's Ministry of Economic Affairs**
- One of Asia's leading **applied technology R&D institutes**
- Incubated top global companies like **TSMC**

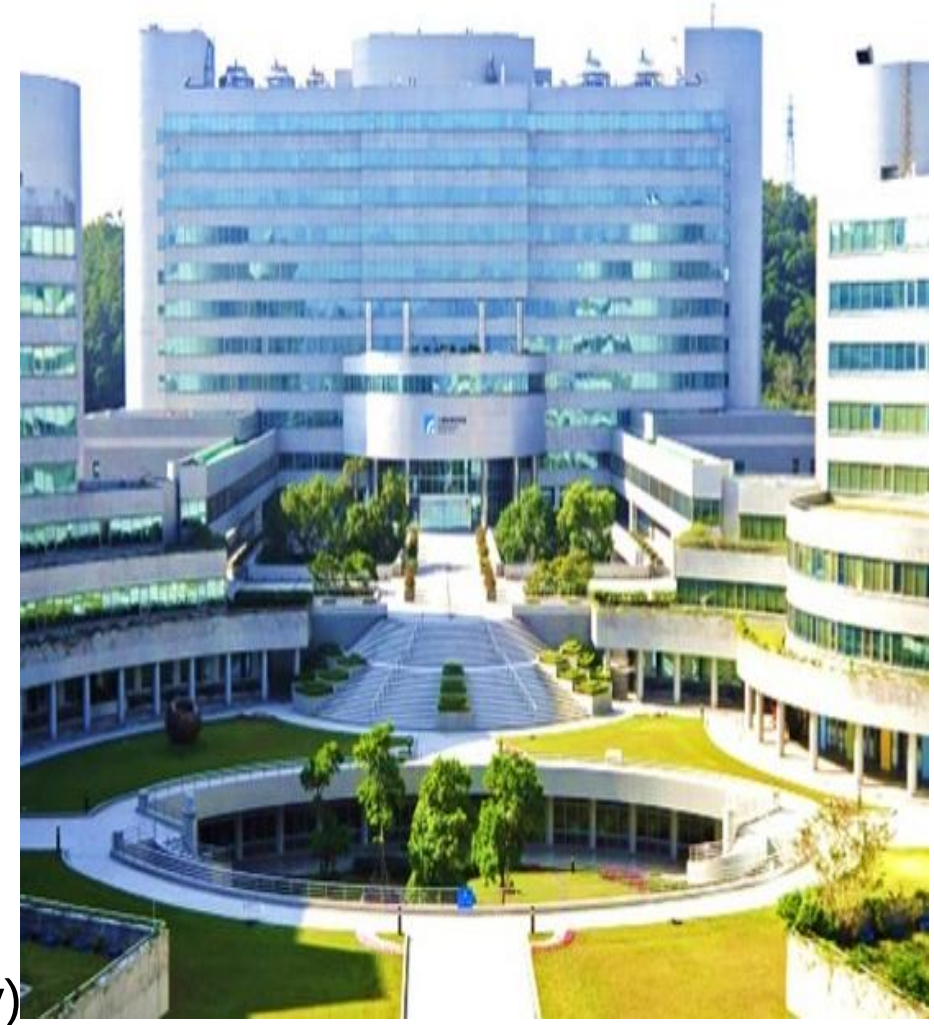
Core Expertise

- **ICT | Semiconductors | Smart Manufacturing**
- **Green Tech | Biomedical | AI & Smart Living**

➢ Driving innovation across **six major tech sectors**

Our Role

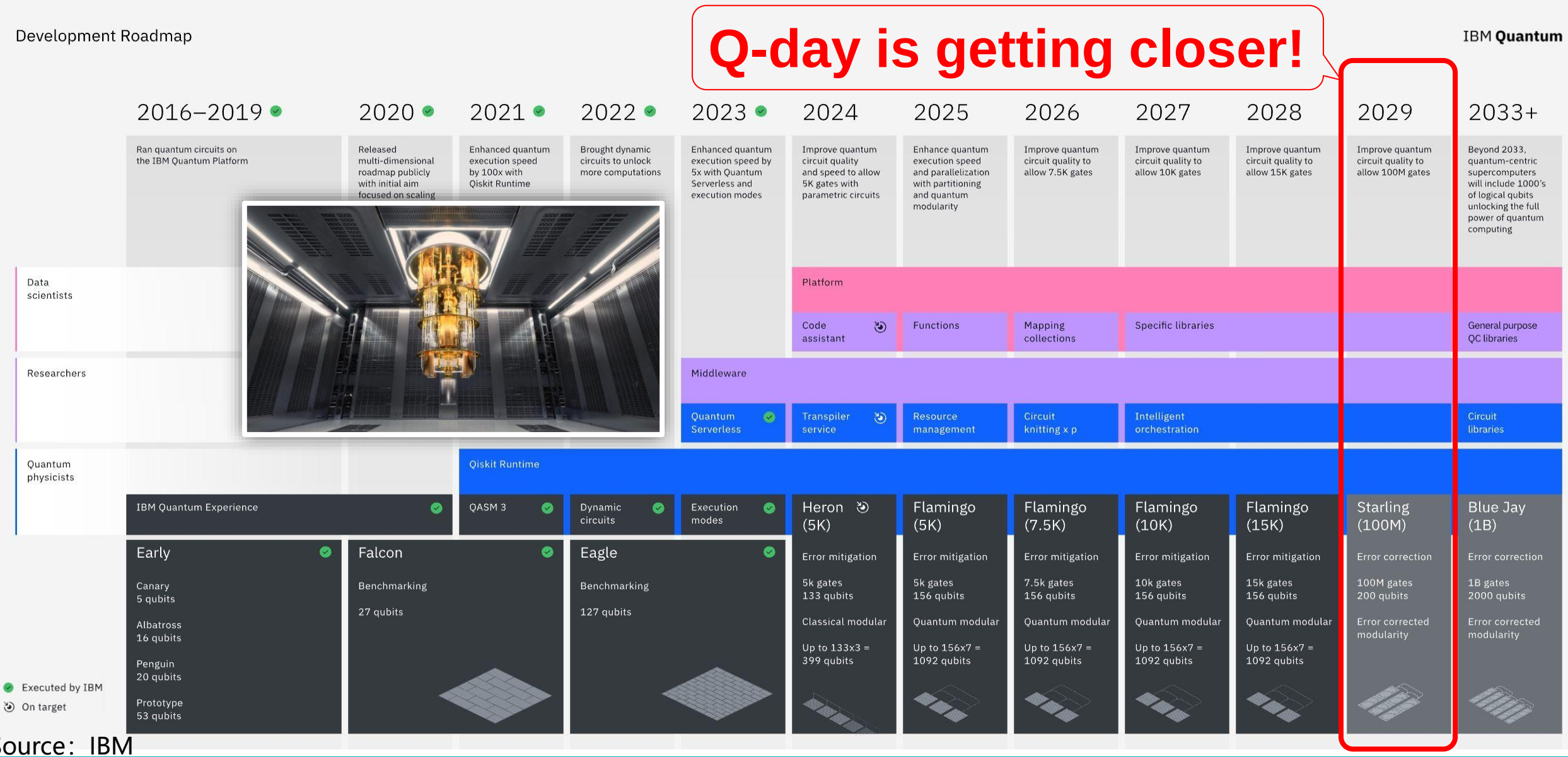
- Bridge **lab to market**
- Support **SMEs' digital transformation**
- Nurture **startups and innovation**
- Partner in **national tech programs** (e.g. Net-Zero, Cybersecurity)



ITRI
Industrial Technology Research Institute

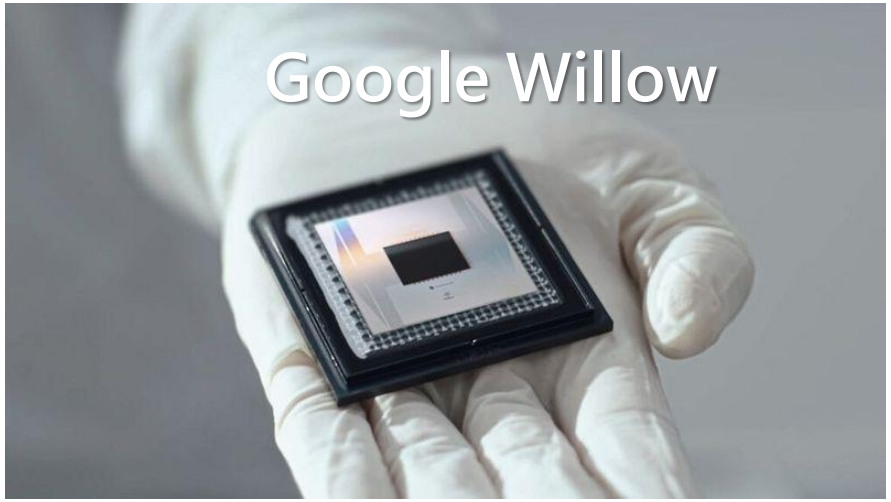
IBM Presents '2029 Million-Qubits' Roadmap

Q-day is getting closer!



Source: IBM

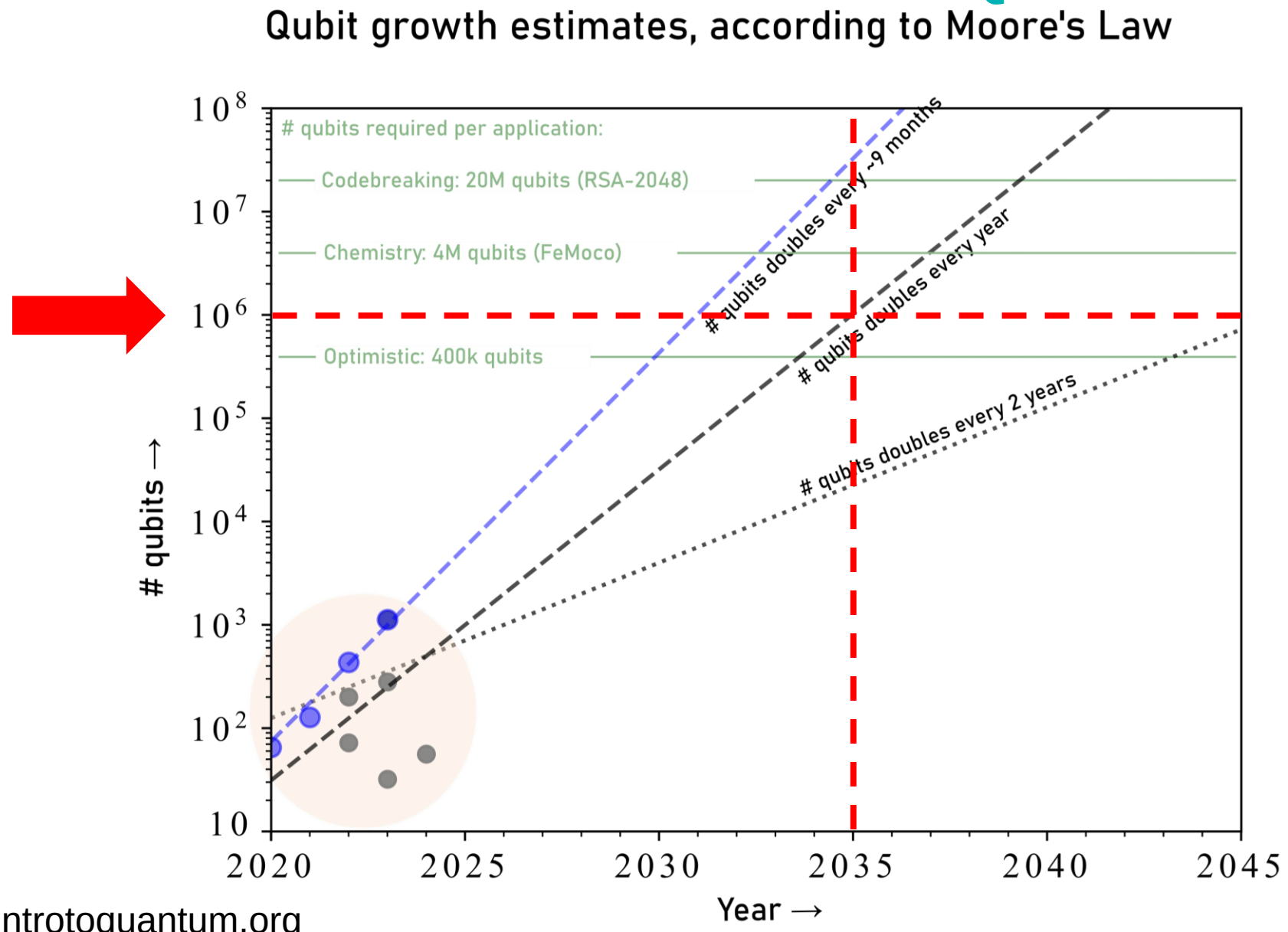
Scaling Qubits with Modular Architecture



Source： **Microsoft, Google, Amazon**

ITRI Industrial Technology Research Institute

Moore's Law : 2035 to See Million-Qubit Breakthrough



Source：introtoquantum.org

Classical Algorithms Challenged: Breaking Time Reimagined

Algorithm	Type	Size of Quantum Computer	Time Required
DL with NIST P-256	Public key	6.8×10^7 Qubits (68M)	1 Day
RSA 3072	Public key	6.4×10^8 Qubits (640M)	1 Day
AES-128	Symmetric	10^{30} Qubits (1G)	1 Year

Shor's algorithm

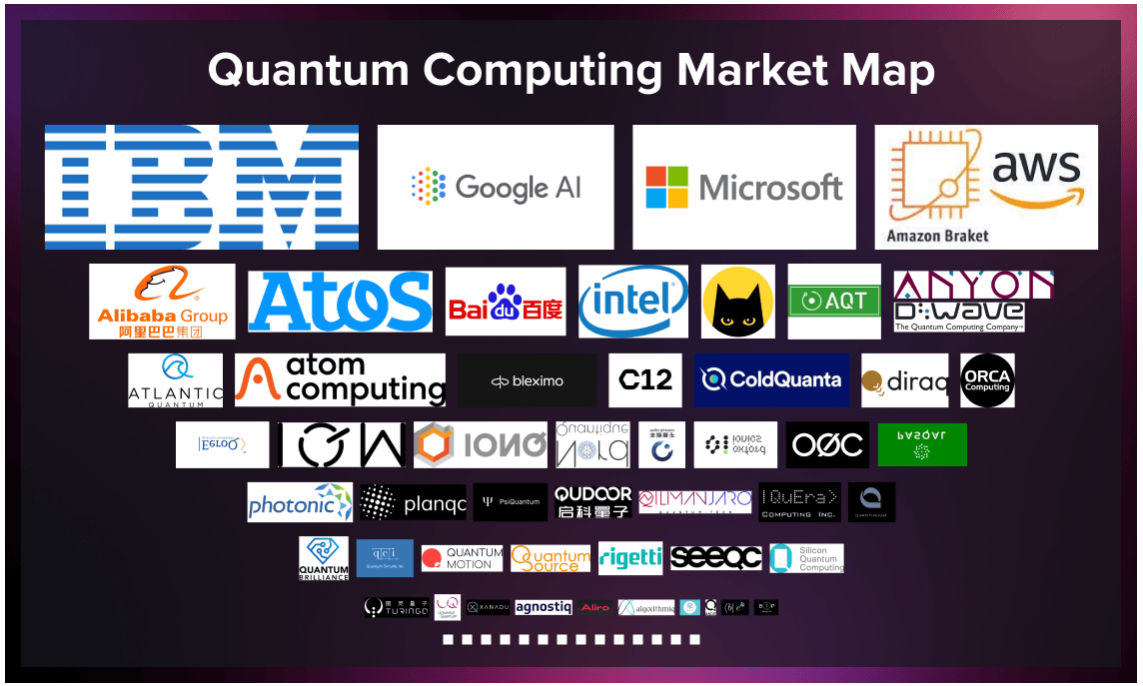
Grover's algorithm

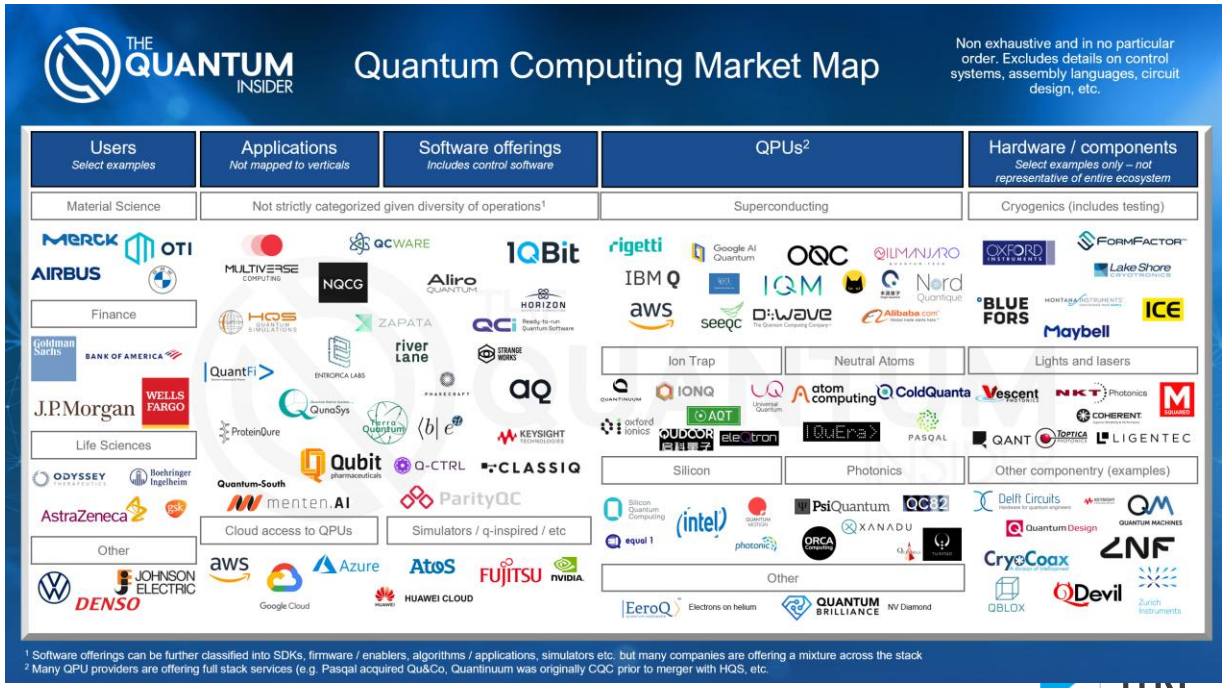
Source：

A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies (IEEE)

Harvest Now, Decrypt Later (HNDL)

Global companies are now involved in building quantum computing solutions—and, of course, even **'hacker applications'** are no exception!





source：serokell.io, thequantuminsider

Progress of NIST PQC Standardization

PQC Algorithm	⭐ ML-KEM (CRYSTALS-Kyber)	⭐ ML-DSA (CRYSTALS-Dilithium)	⭐ SLH-DSA (SPHINCS+)	FN-DSA (Falcon)	NEW HQC (Hamming Quasi-Cyclic)
FIPS Standard	FIPS 203	FIPS 204	FIPS 205	FIPS 206 (Delayed)	Planned
Type	Key Encapsulation	Digital Signature	Digital Signature	Digital Signature	Key Encapsulation
Cryptography	Lattice-based	Lattice-based	Hash-based	Lattice-based	Code-based
Key Characteristics	• NIST's primary KEM standard • Good cross-platform performance • Relatively compact key sizes; fast operations • Efficient in both encryption and decryption • Suitable for embedded and IoT devices	• NIST's primary digital signature standard • Moderate key/signature sizes; fast signing and verification • Good security-performance balance • Suitable for high-performance and low-resource applications	• Alternate signature standard • Based on hash functions, highly reliable security • Large signature size, spatially limited • Stateless and security-stable	• Small signatures and public keys • Low bandwidth, fast verification • Complex key/signature generation (may involve floating-point ops) • Complex to implement; needs further validation for stability and side-channel resilience	• Candidate for code-based encryption • High computational overhead; best suited for high-resource environments • Large key sizes; unsuitable for low-power devices
Standardization Timeline	Finalized in August 2024			Final draft of FIPS 206 expected post-2025	Draft expected ~2026 Final ~2027 (tentative)

Source: Topology Research Institute (TRI), compiled by ITRI, May 2025

ITRI Industrial Technology Research Institute

Challenges of PQC Applications R&D

PQC Algorithm is Difficult

No Reference Design

Interoperability Testing

Budget

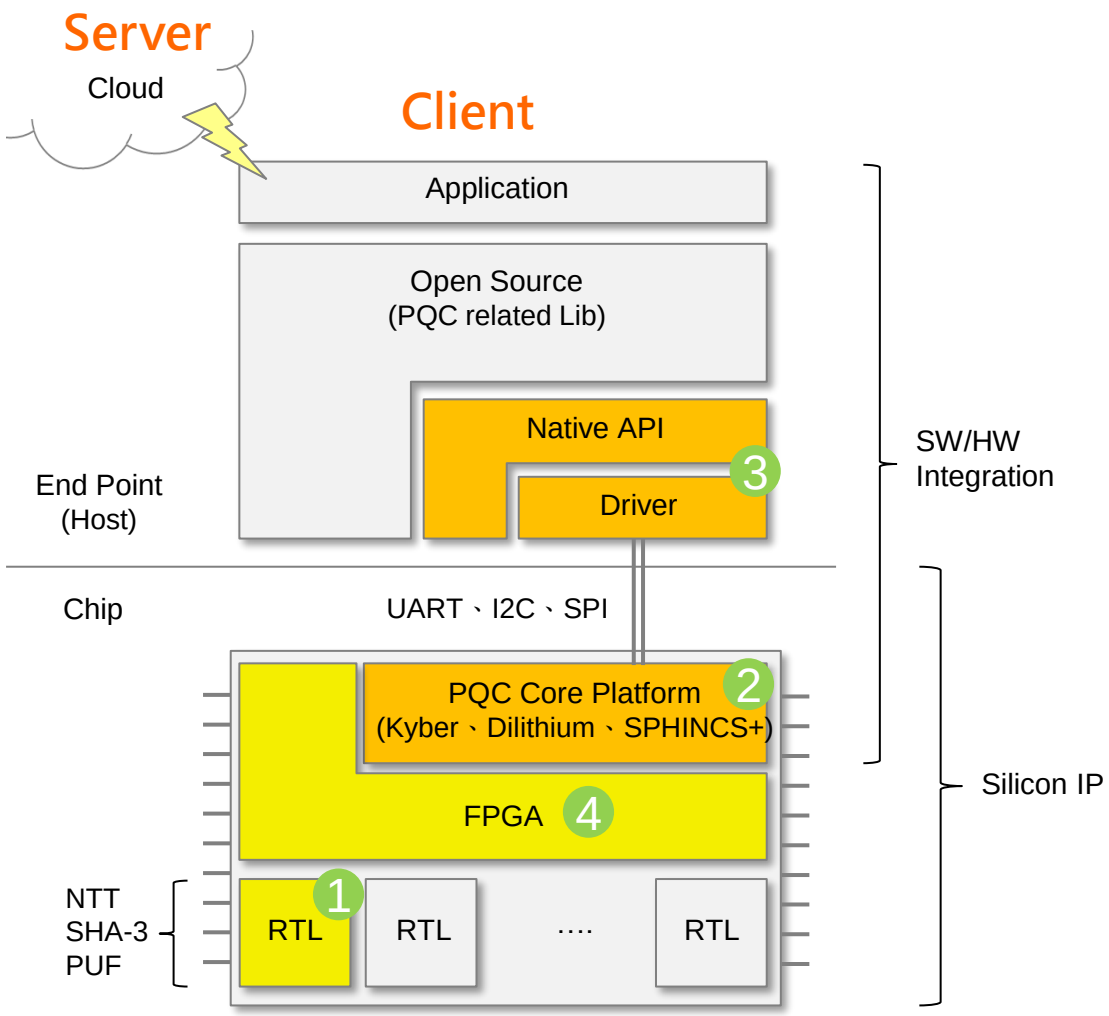
Lowering the Barriers: PQC Common Platform

1. **Deployment of PQC on Both Server and Client →**
   Provides a standard RTL circuit interface for integrating complete PQC algorithms or partial accelerator components.

2. **Complexity of PQC Security Architecture →**
   Offers PQC Core Algorithm Platform with NIST standardized algorithms to facilitate digital logic design verification.

3. **Challenges of PQC Algorithm Libraries→**
   Provides corresponding firmware algorithm libraries and APIs for easy industry application integration.

4. **High Development Costs of ASIC Chips→**
   Provides FPGA verification environment to assist in the feasibility validation of silicon IP and supports specialized chip product design.



PQC Common Platform and Application Use Cases

The PQC Common Platform Solution includes four key components: PQC Silicon Intellectual Property, PQC Software and Firmware, PQC Chip Design and Verification Environment, and PQC Application Reference Examples.

PQC Application Reference Examples.
(Identification、Digital Signature)

PQC Chip Common Platform for Product Design and Verification Environment (FPGA)

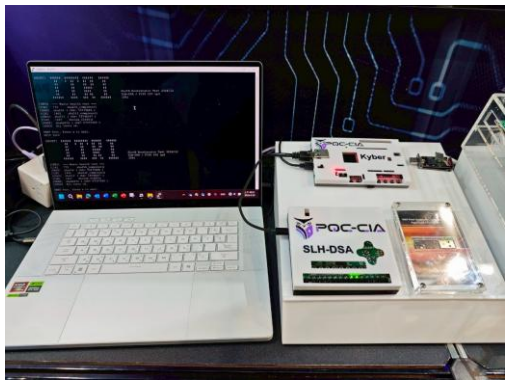
PQC IP
ML-KEM(Kyber) 、
ML-DSA(Dilithium)、
SLH-DSA(SPHINCS+)

PQC SW/FW
ARM、RISC-V、
X86 、...

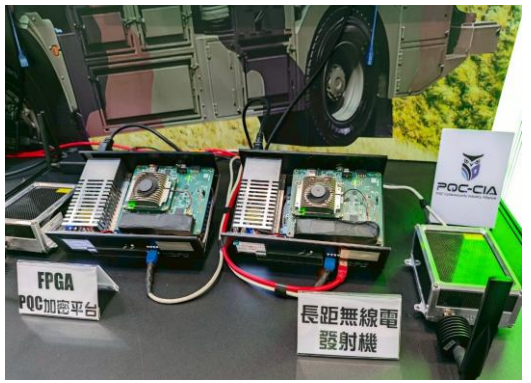
All of the above are ready for collaboration

Identification

Digital Signature



PQC IP & PQC SW/FW



PQC Chip Common Platform

ITRI Industrial Technology Research Institute

PQC Applications
(Identification、Digital Signature)

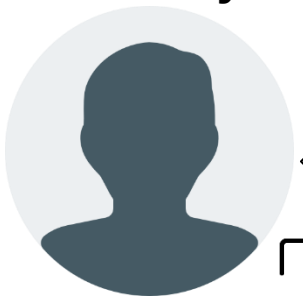
ITRI
Industrial Technology
Research Institute

ITRI Identity Authentication Solution

FIDO2@PQC Authenticator

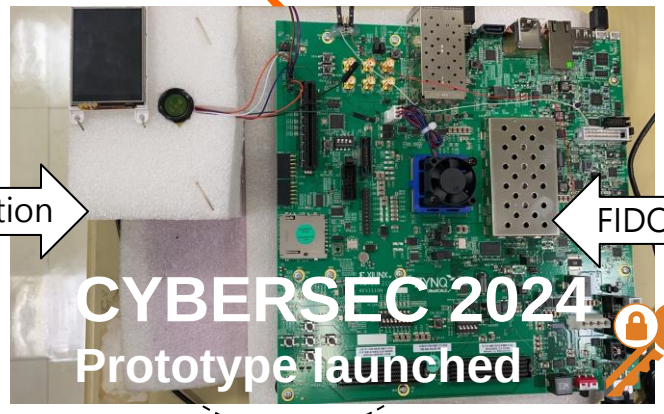
FIDO2@PQC Server

Fast Identity Online



User Identification

User verification



FIDO2 CTAP2

Challenge

FIDO2 Webauthn

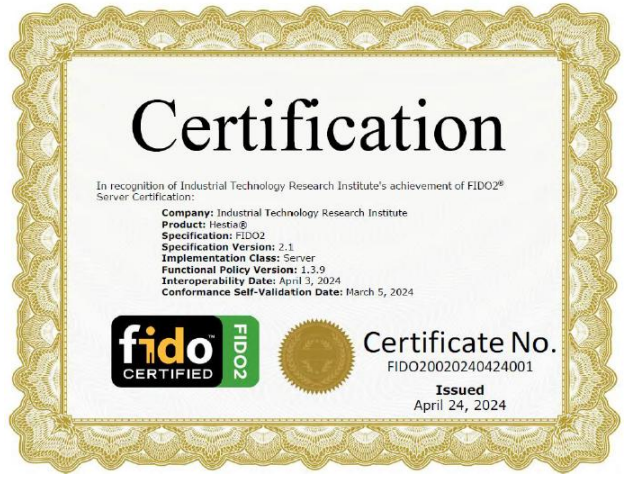
FIDO2 Server

Response

Require user identification before private key can be used

Dilithium Private key (handle) per account

Dilithium Public key



ITRI Industrial Technology Research Institute

ITRI E-Signature Service Solution

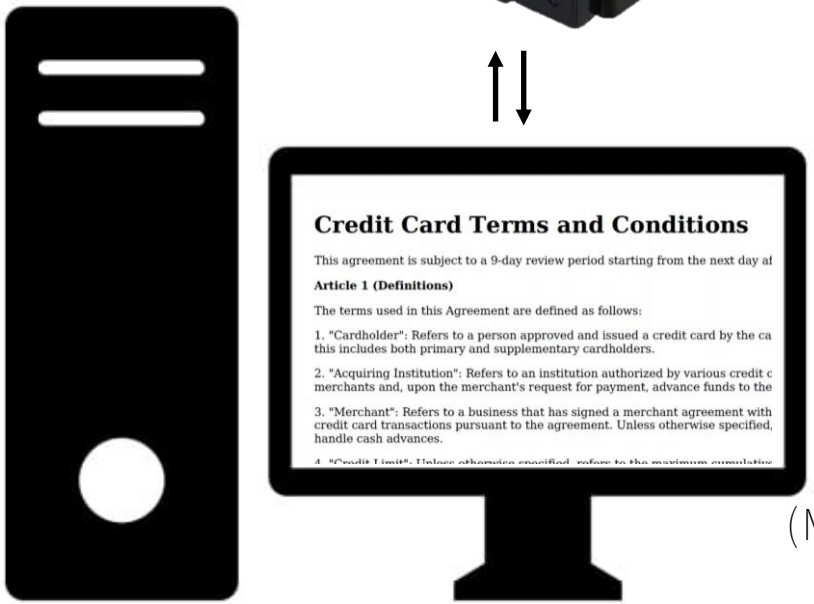
*PQC HSM

*PQC Data Diode

*PQC Hybrid PIV Dongle
(FIDO2/PKI)

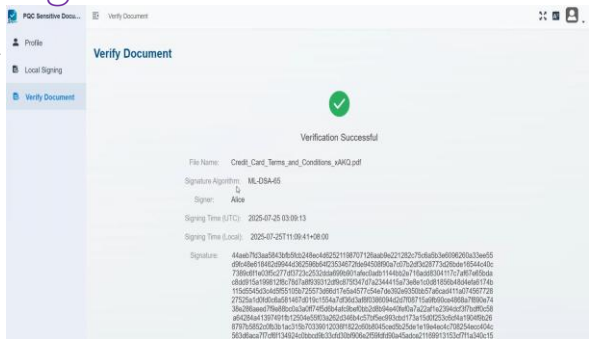
(ML-DSA)Key Generation / Signature

(ML-DSA)User Authentication and Authorization



PQC Tunnel(ML-KEM)

Signature Audit Service



(ML-DSA)Verify signature

Authentication and e-Signature Services

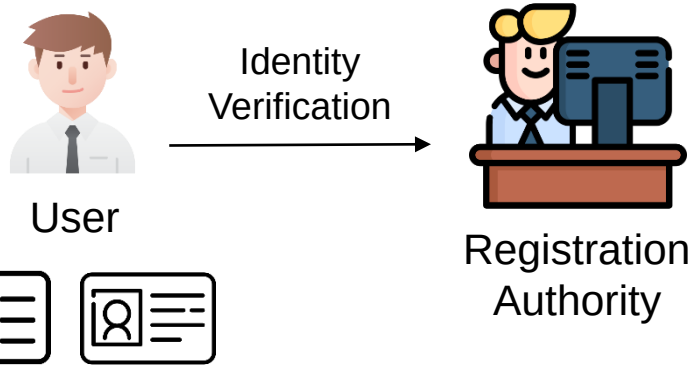
Collaborative Partner	
Product Item	**Company Name**
PQC Hybrid PIV Token	AuthenTrend Technology Inc
PQC HSM	CHT Security Co., Ltd.
PQC Data Diode	Zyell Solutions Corporation

ITRI E-Signature Server (Fast Agree)

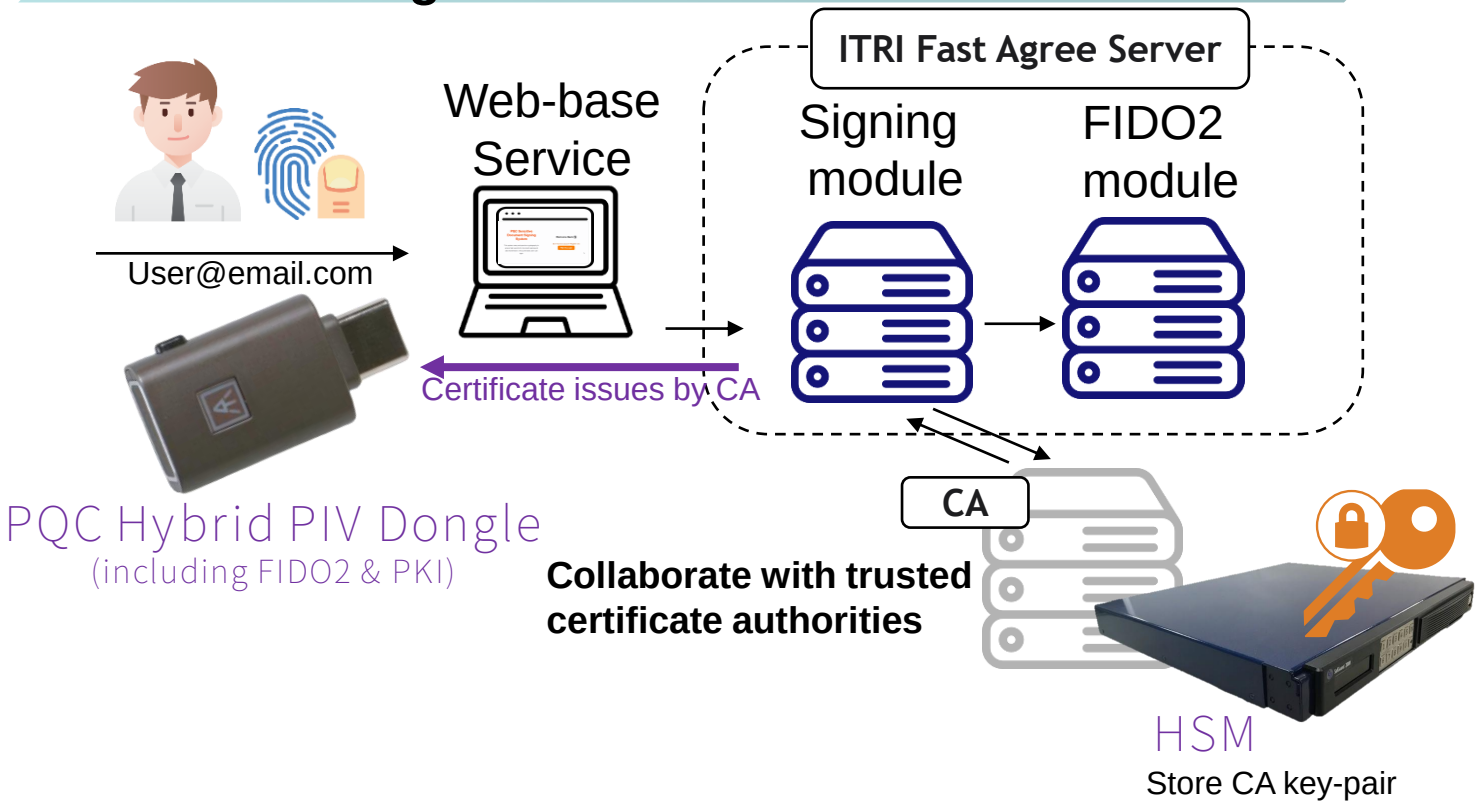
ITRI Industrial Technology Research Institute

E-Signature System: Registration Process

Physical KYC for Customer Verification



Secure Digital Identity Enrollment and Certificate Provisioning



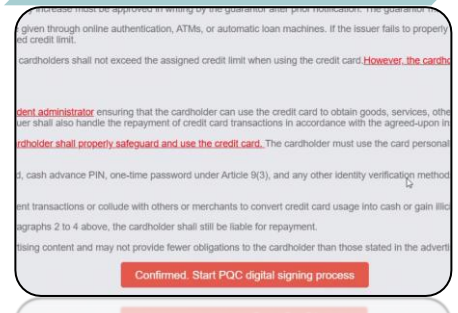
After completing dual ID verification, the user registers with "Fast Agree" , obtains a digital certificate that issues by CA, and securely stores the user's private key and certificate in the PQC Hybrid PIV Dongle.

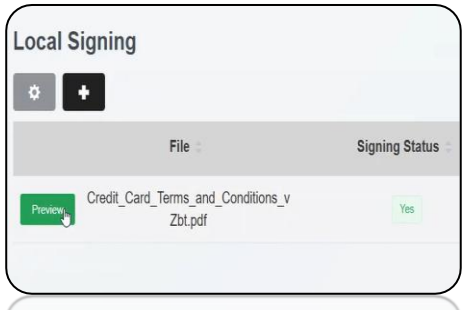
ITRI Industrial Technology Research Institute

E-Signature System: Signing Process

support (ML-DSA-65 and ECC-P256 Signature)

Login → **Select a document** → **Review** → **Signing** → **Finish**





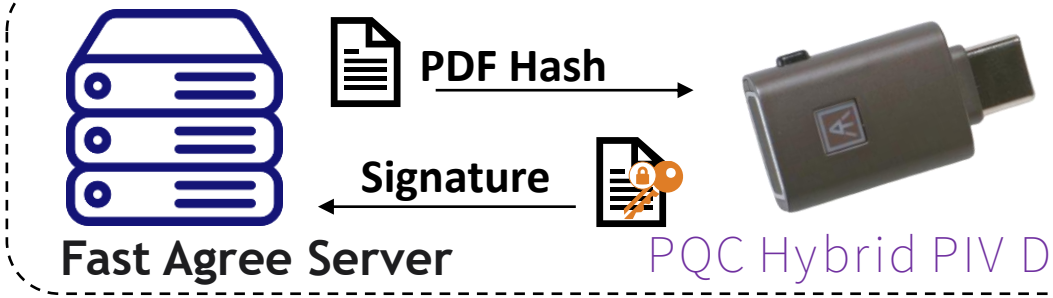
PQC Hybrid PIV Dongle
(including FIDO2 & PKI)

PQC Hybrid PIV Dongle
(including FIDO2 & PKI)

signature performance

Algorithm	Signature Time (ms)
ML-DSA-65	830.04
ECC-P256	658.47

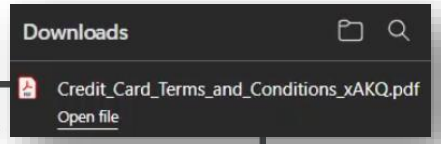
User logs in with fingerprint, picks a document, checks it, and signs with a PQC Hybrid PIV Dongle. It supports both ML-DSA65 and traditional ECC-P256 signature.

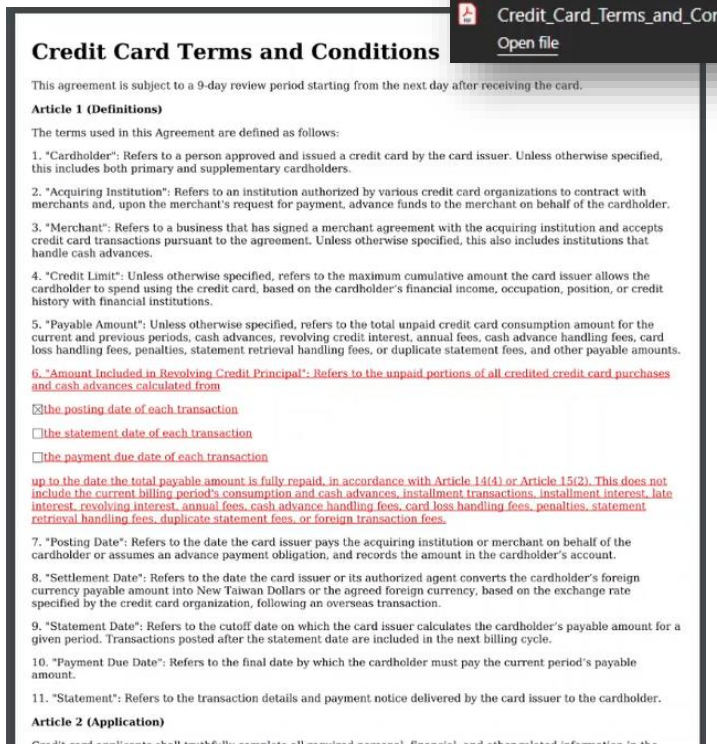


ITRI Industrial Technology Research Institute

E-Signature System: Two Verification Process

Download signed document





Credit Card Terms and Conditions

This agreement is subject to a 9-day review period starting from the next day after receiving the card.

Article 1 (Definitions)

The terms used in this Agreement are defined as follows:

1. "Cardholder": Refers to a person approved and issued a credit card by the card issuer. Unless otherwise specified, this includes both primary and supplementary cardholders.

2. "Acquiring Institution": Refers to an institution authorized by various credit card organizations to contract with merchants and, upon the merchant's request for payment, advance funds to the merchant on behalf of the cardholder.

3. "Merchant": Refers to a business that has signed a merchant agreement with the acquiring institution and accepts credit card transactions pursuant to the agreement. Unless otherwise specified, this also includes institutions that handle cash advances.

4. "Credit Limit": Unless otherwise specified, refers to the maximum cumulative amount the card issuer allows the cardholder to spend using the credit card, based on the cardholder's financial income, occupation, position, or credit history with financial institutions.

5. "Payable Amount": Unless otherwise specified, refers to the total unpaid credit card consumption amount for the current and previous periods, cash advances, revolving credit interest, annual fees, cash advance handling fees, card loss handling fees, penalties, statement retrieval handling fees, or duplicate statement fees, and other payable amounts.

6. "Amount Included in Revolving Credit Principal": Refers to the unpaid portions of all credited credit card purchases and cash advances calculated from

☒the posting date of each transaction

☐the statement date of each transaction

☐the payment due date of each transaction

up to the date the total payable amount is fully repaid, in accordance with Article 14(4) or Article 15(2). This does not include the current billing period's consumption and cash advances, installment transactions, installment interest, late interest, revolving interest, annual fees, cash advance handling fees, card loss handling fees, penalties, statement retrieval handling fees, duplicate statement fees, or foreign transaction fees.

7. "Posting Date": Refers to the date the card issuer pays the acquiring institution or merchant on behalf of the cardholder or assumes an advance payment obligation, and records the amount in the cardholder's account.

8. "Settlement Date": Refers to the date the card issuer or its authorized agent converts the cardholder's foreign currency payable amount into New Taiwan Dollars or the agreed foreign currency, based on the exchange rate specified by the credit card organization, following an overseas transaction.

9. "Statement Date": Refers to the cutoff date on which the card issuer calculates the cardholder's payable amount for a given period. Transactions posted after the statement date are included in the next billing cycle.

10. "Payment Due Date": Refers to the final date by which the cardholder must pay the current period's payable amount.

11. "Statement": Refers to the transaction details and payment notice delivered by the card issuer to the cardholder.

Article 2 (Application)

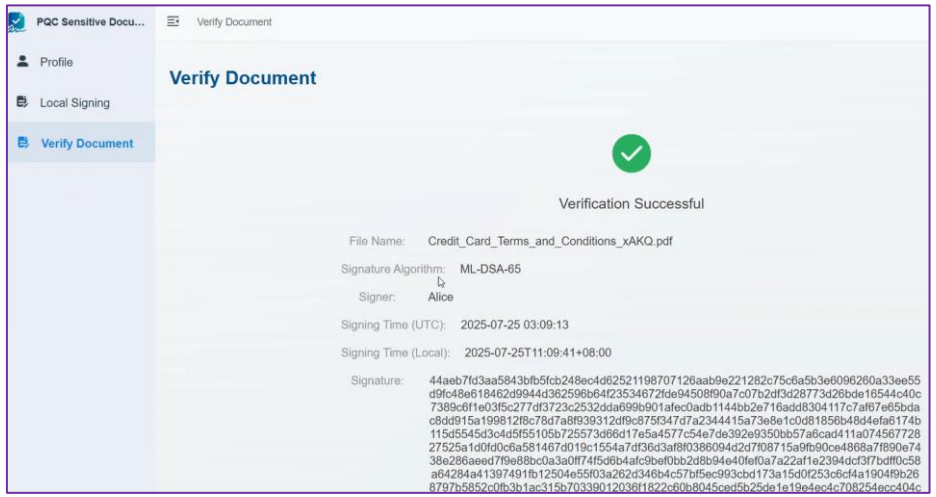
Upload signed document to verify with web-based verification tools

Note1: Signed using ML-DSA

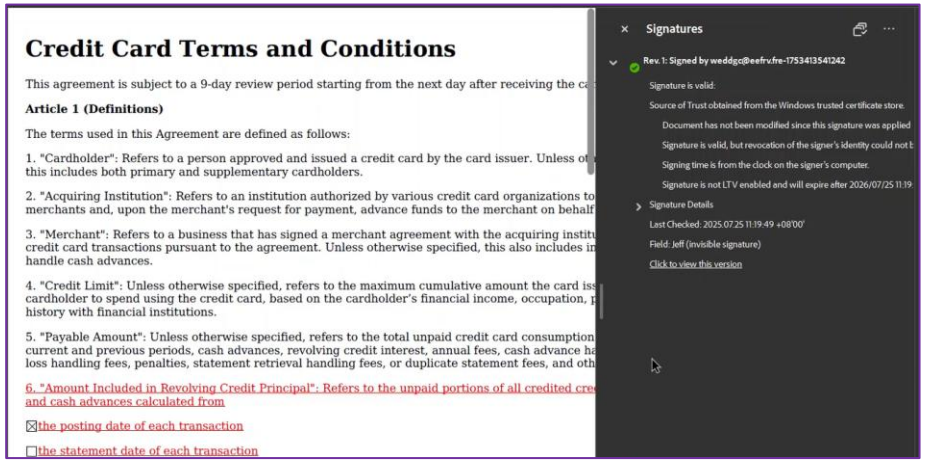
Open File with PDF Reader

Note2 Signed using traditional cryptographic algorithms (ECC-P256)

web-based verification tools



PDF reader verification



Users can verify signed documents using PDF Reader, or through the web-based verification tool provided within Fast Agree.

ITRI Industrial Technology Research Institute

ITRI PQC E-Signature Solution Demo

Using the PQC-Enabled Security Dongle

https://www.youtube.com/watch?v=TJ5tDWpnxGs

ITRI
Industrial Technology Research Institute

Derek Chen Technical Manager

Application Integration Technology Dept.
Division for Infra & Cyber Security
Information and Communications Research Laboratories

9F., No.315, Songjiang Rd., Zhongshan Dist.,
Taipei City 104070, Taiwan, R.O.C.
Tel：+886 2 2515 9665 ext. 161
Mobile：+886 973 301838
E-mail：derekchen@itri.org.tw

www.itri.org.tw

THANKS FOR YOUR LISTENING

Inquiries on PQC, e-signatures, or PIV dongles are welcome.

ITRI
Industrial Technology Research Institute