

工業技術研究院

Industrial Technology
Research Institute



Taipei PKI Progress : Enabling Industry PQC Applications Through PQC Common Platform

Tsai Yi-Chang Technical Manager

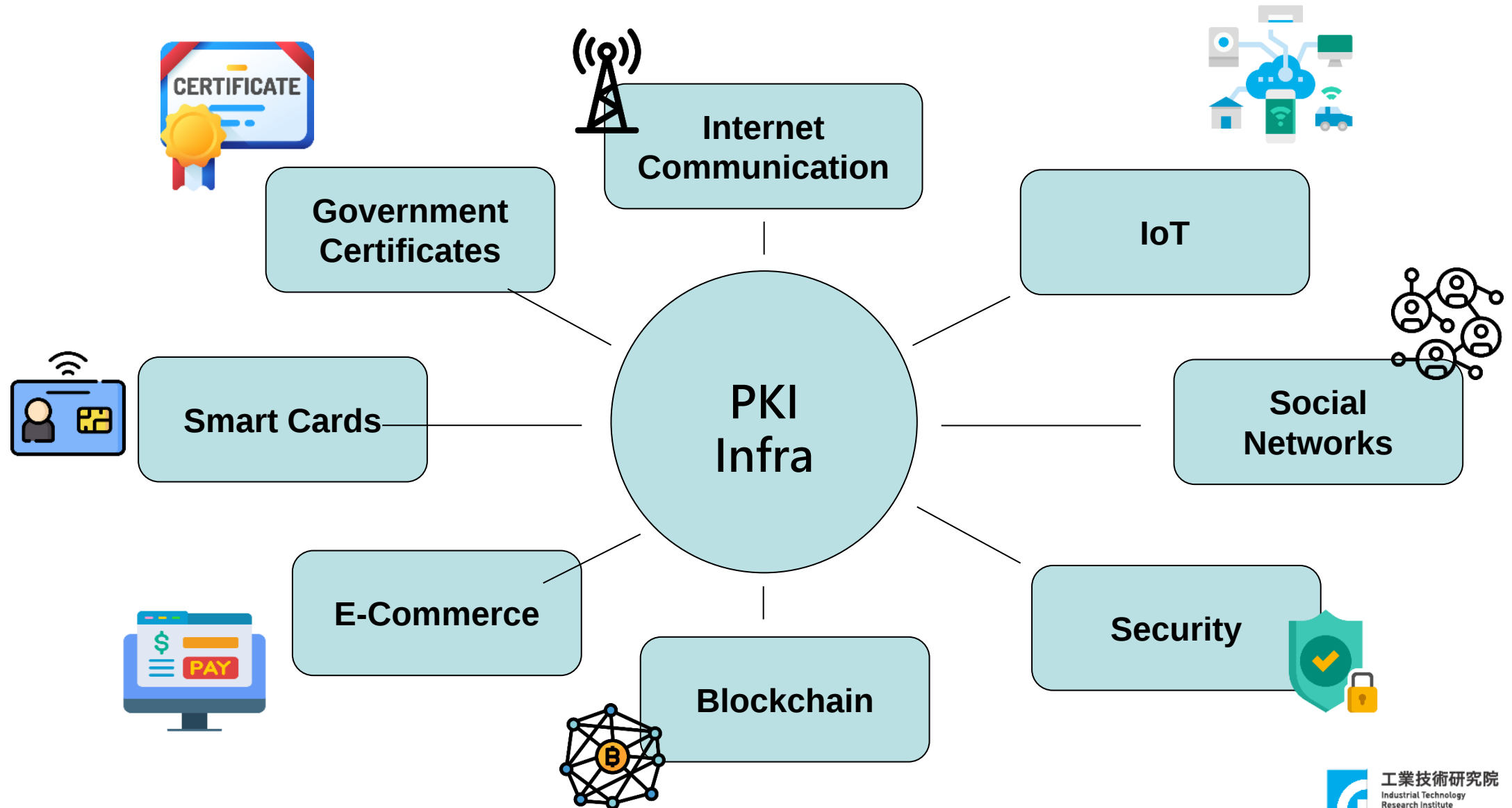
Industrial Technology Research Institute (ITRI)
Information and Communications Research Laboratories
2024/06/13

Q-Day Is Approaching, and Traditional Encryption Algorithms Are Facing Challenges!

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SAH-2, SHA-3	-	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Source : NIST IR 8105, ITRI (2024)

Wide Applications of PKI



Post-Quantum Cryptography (PQC)

NIST PQC Standardization (R4)

**CRYSTALS-
Kyber**

**CRYSTALS-
Dilithium**

Falcon

SPHINCS+

KEM

Signatures

Lattice

Hash

PQC Algorithm Basic Types

Lattice

Hash

Code

Multivariate

Major Companies Adopting PQC to Prevent 'Harvest Now, Decrypt Later'!

Apple: Uses PQC encryption in iMessage, with unique keys for each message.

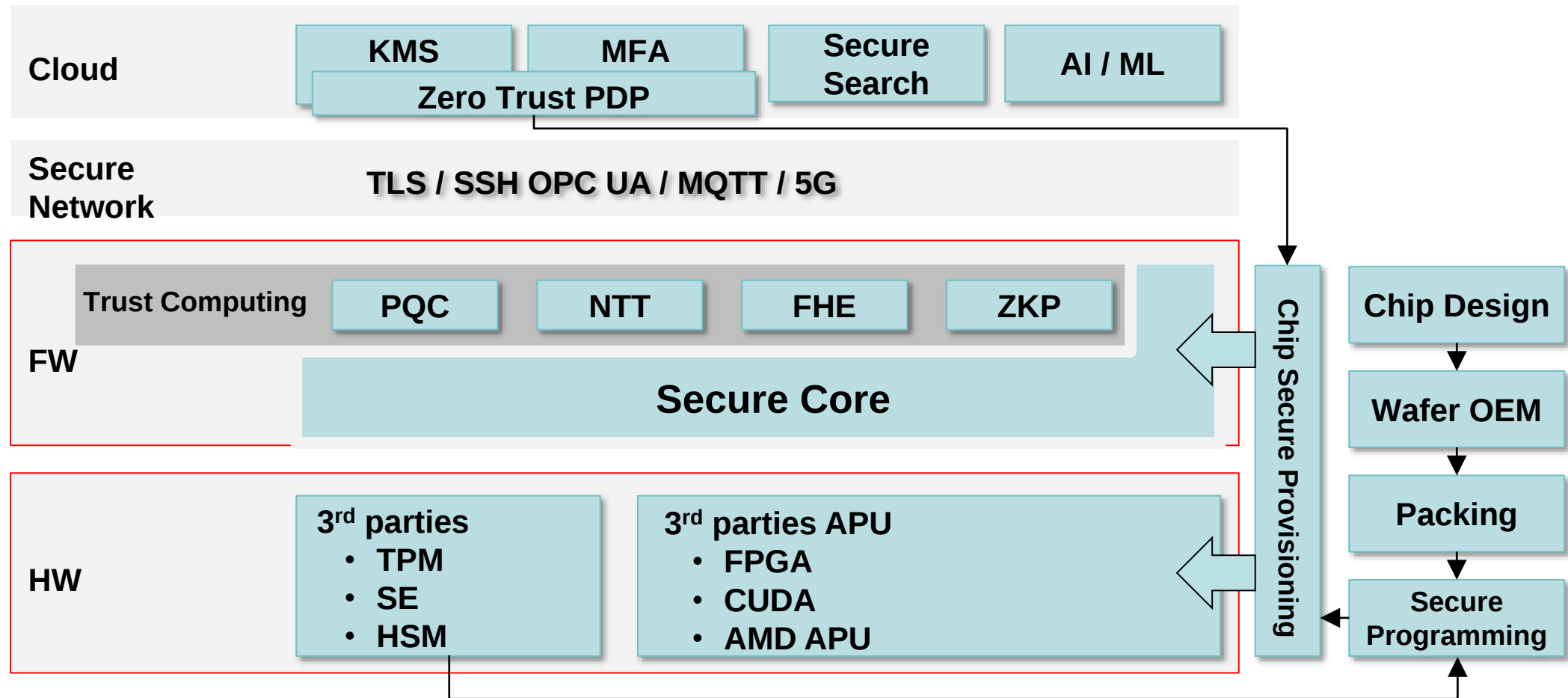


Google : Chrome 116 implements PQC-based FIDO2 Security key.



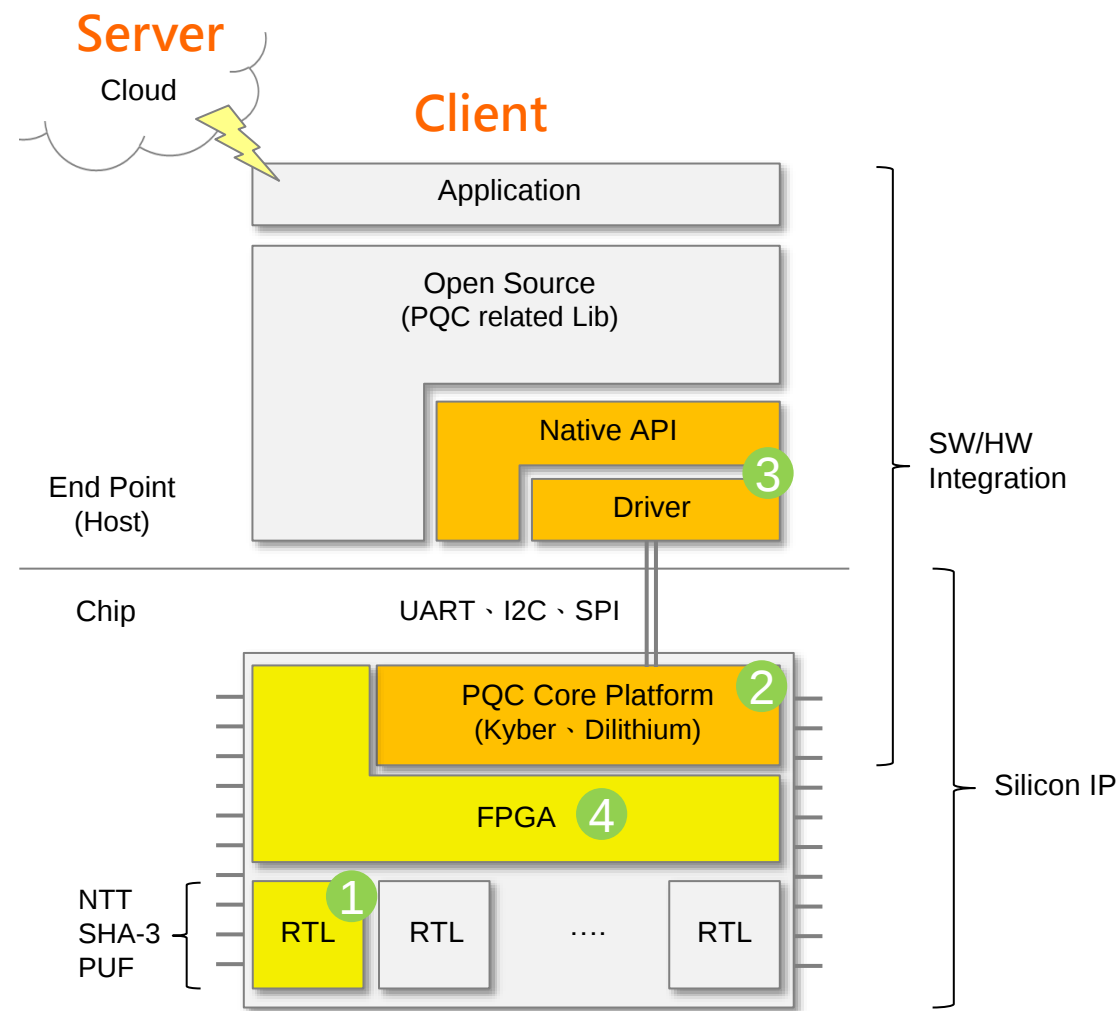
Source : forbes,certera, ITRI (2024/06)

Quantum Security Relies on the Integration of Post-Quantum Safe Software and Hardware

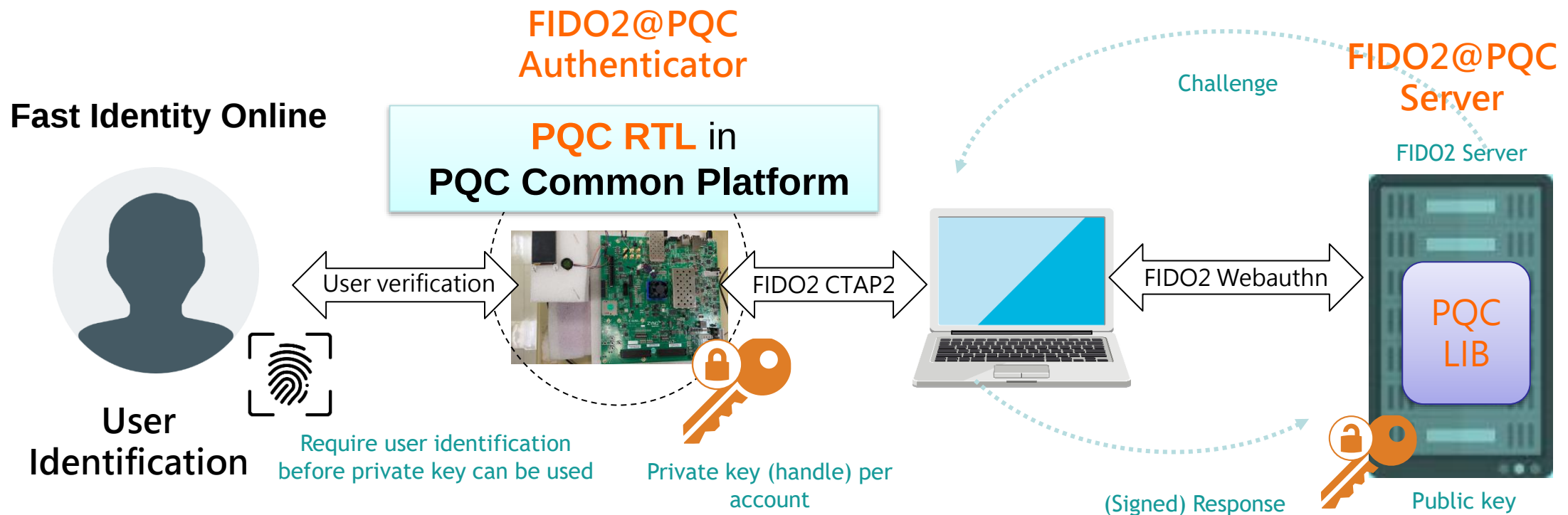


Lowering the Barriers: PQC Common Platform

- 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.

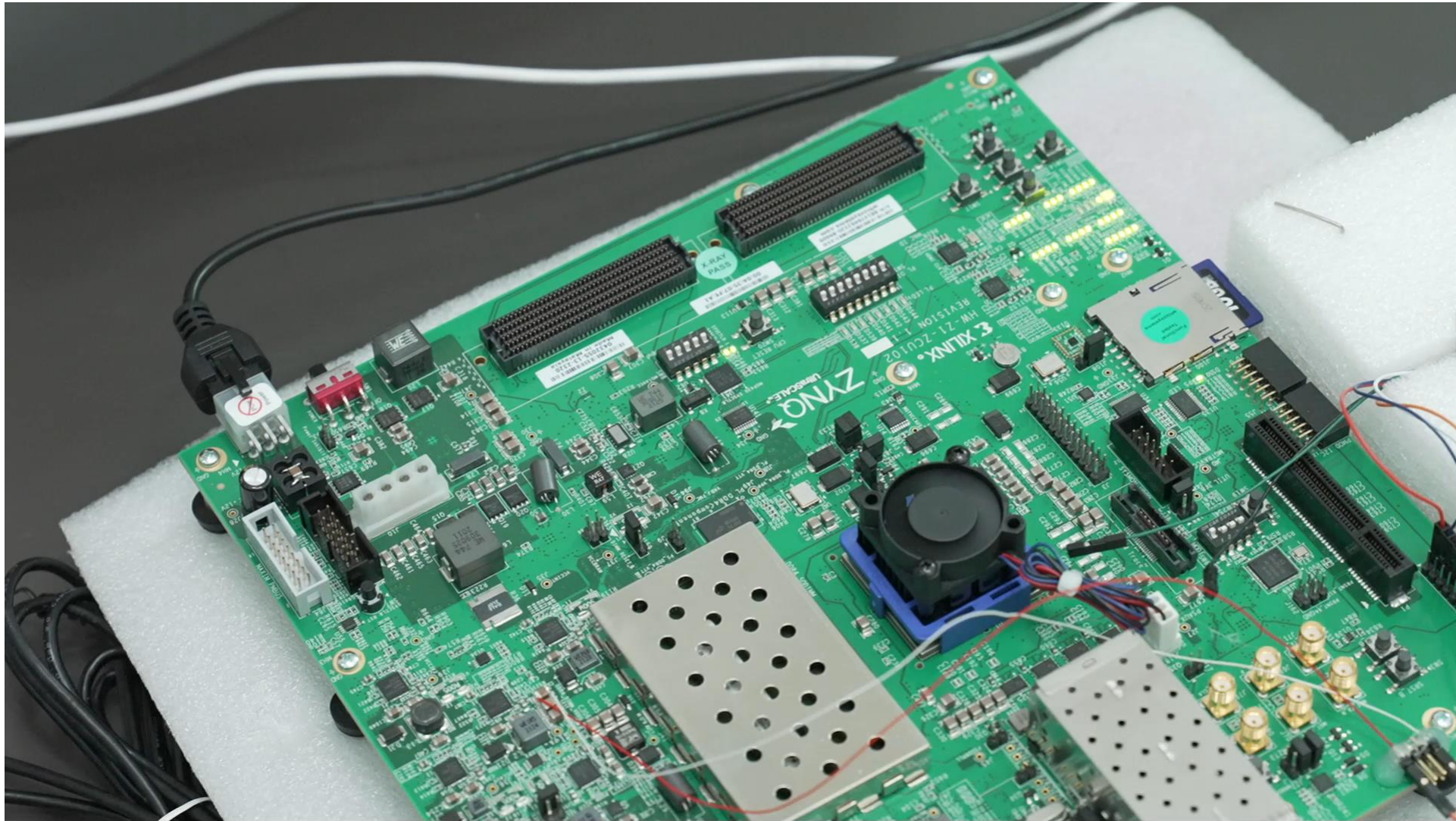


Use Case: Developing FIDO2@PQC with PQC Common Platform



ITRI FIDO2 Authentication with PQC protection

The Use Case Demo Video



Thanks