CYBERSEC 2025 臺灣資安大會 | 4/15-4/17 臺北南港展覽二館

AIoT&Hardware SECURITY ZONE

AIOT & HARDWARE SECURITY SUMMIT

Securing the Future – Post-Quantum ZTA with Dynamic PUF Root-of-Trust

TEAM CYBERSECURITY

智能資安科技股份有限公司

Nicolas FAHIER

Intelligent Information Security Technology Inc.

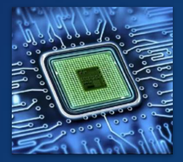
Chief Technology Officer

About IIST Inc.

PUF-based dynamic Root-of-Trust Solutions

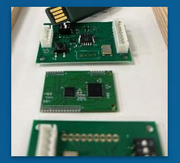
Securing Digital Lives , Tackling Modern Security Challenges

Security Silicon IPs



Security IC Chips

Security Modules



System Integration

ACADEMIC-INDUSTRY COLLABORATION EXCELLENCE

IIST Inc. History

Born from groundbreaking research at National Yang Ming Chiao Tung University. Specializing in advanced chip security and system integration, we’ ve spent years pushing the boundaries of innovation to redefine what digital security means. Our team has worked tirelessly to translate academic excellence into practical, cutting-edge solutions that address real-world hardware security challenges.

2020

NYCU 陽明交通大學

Innovative PUF Design

R&D Proof-of-Concept

2021

國科會 & 經濟部

NSC & MOE

Creation plans fundings

2023

公司設立

Company established and operating in Hsinchu Science Park

2024

市場進入

Market Entry with first PUF IC, Module and Security USB Key

CYBERSEC 2025
臺灣資安大會

Market Context

New Cybersecurity Paradigm

Challenges & Problems are multiplying

IIST

New Cybersecurity Paradigm

AIoT&Hardware SECURITY ZONE

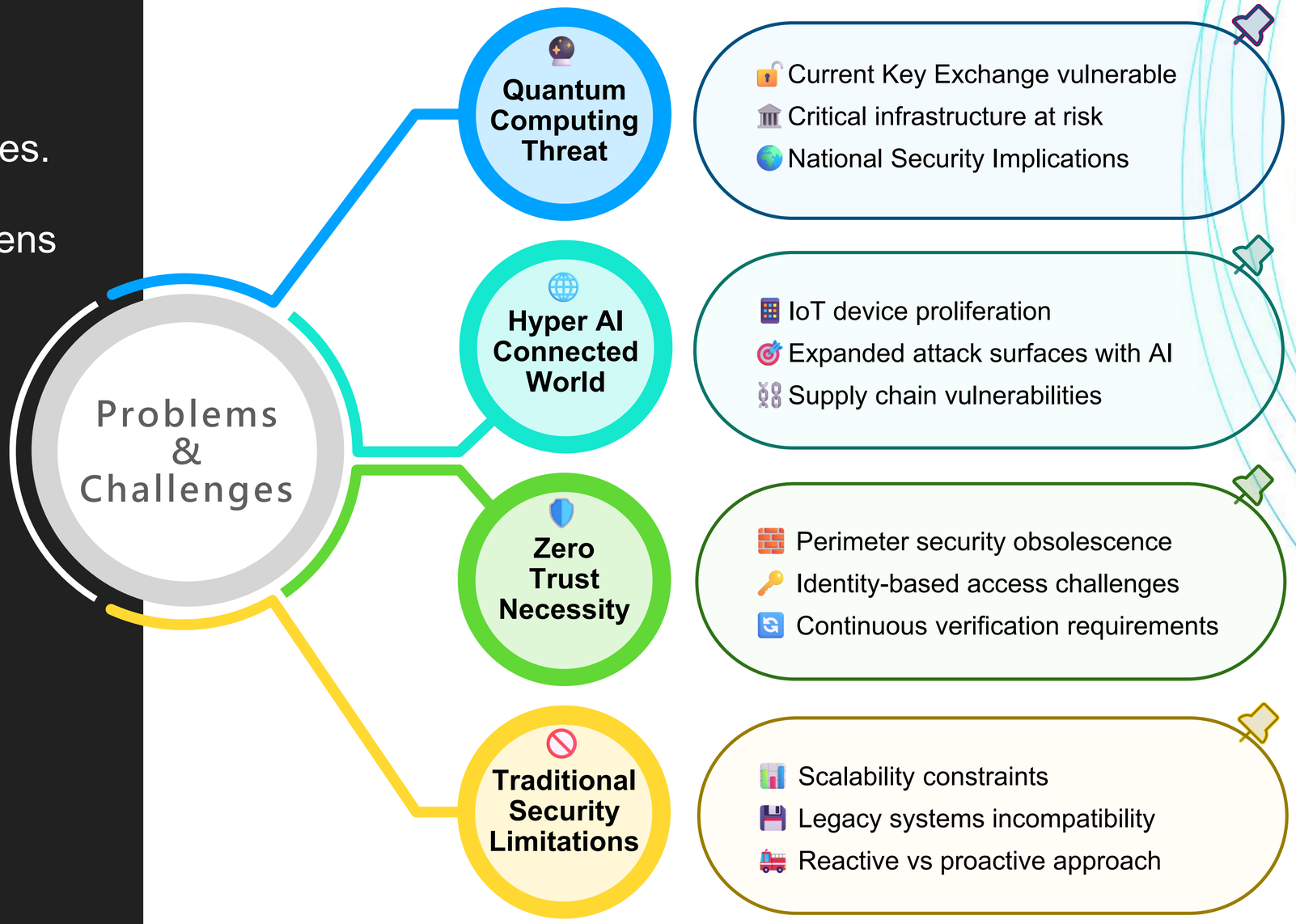
IoT expansion, Zero Trust adoption, and our hyper AI connected world create unprecedented vulnerabilities.

Quantum computing threatens our encryption foundations.

Traditional security approaches can no longer protect against these emerging challenges.

The future demands innovative solutions.

Evolving Landscape & Threats



CYBERSEC 2025
臺灣資安大會

Building IT & OT

Post-Quantum & Zero-Trust

Next cybersecurity challenge

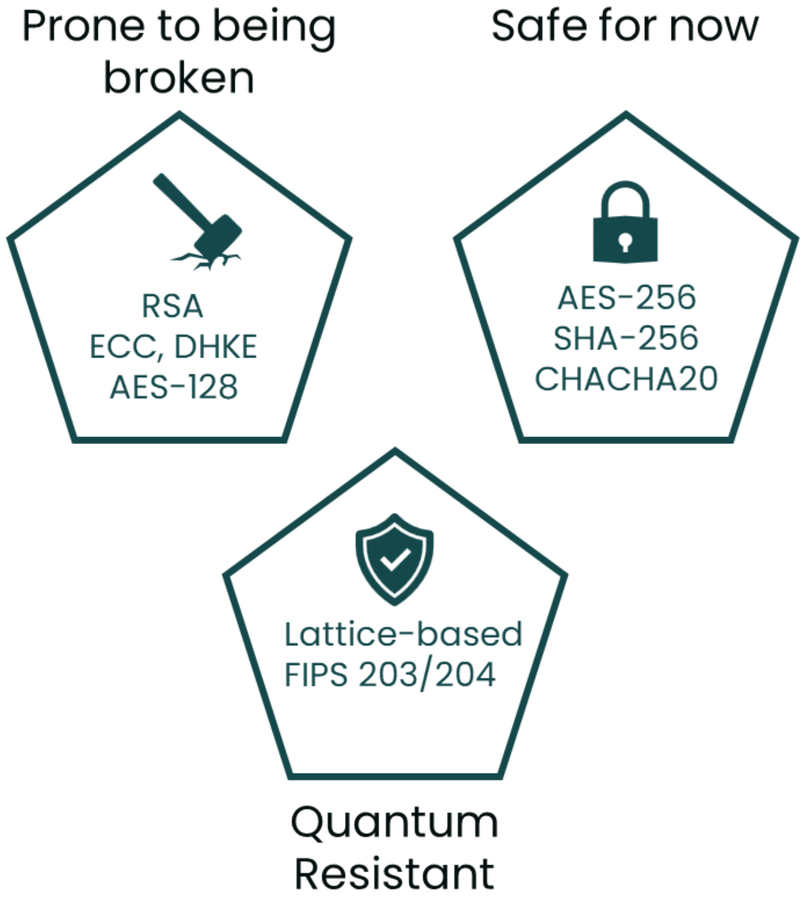
🔍 Post-Quantum Computing Threat

Threat to Traditional Cryptography

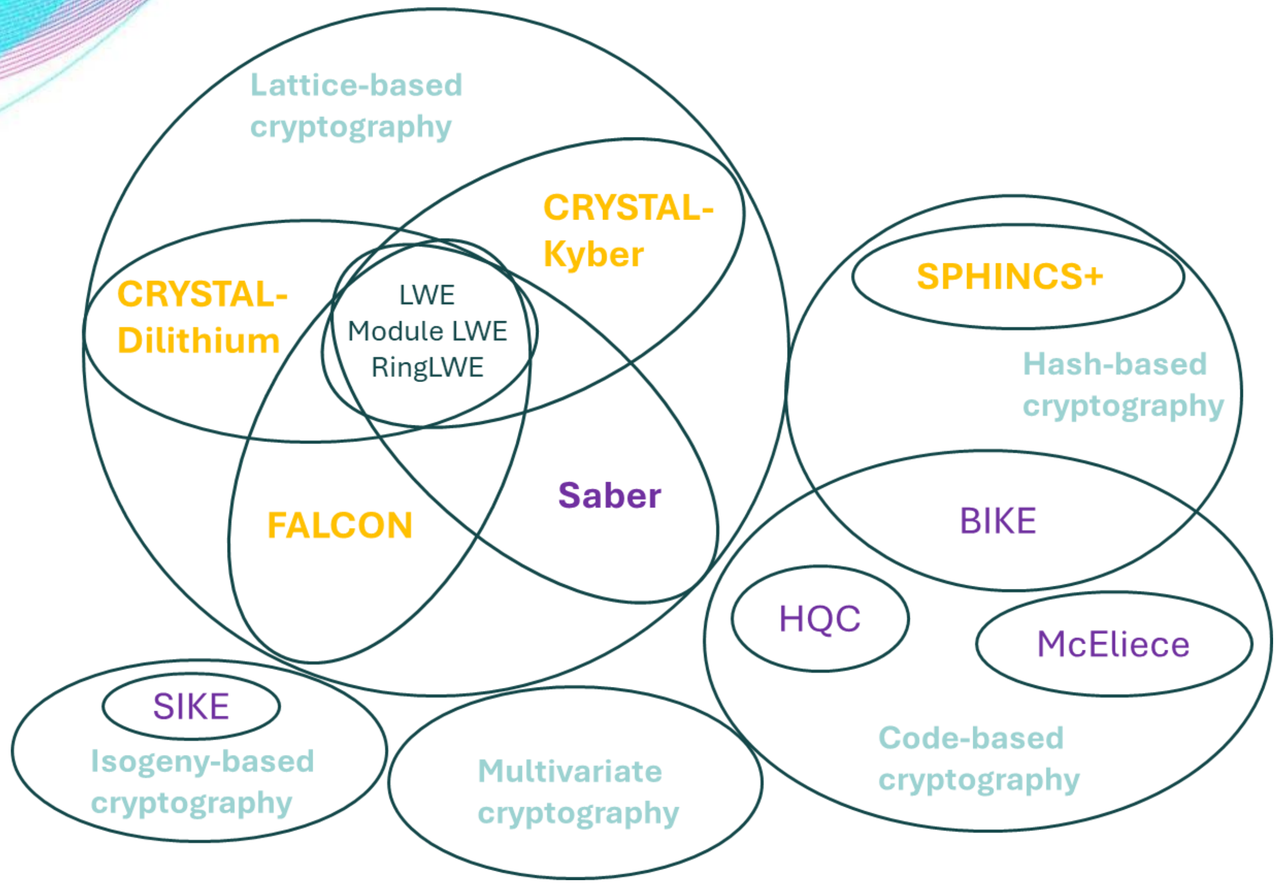
Impact of quantum computing

Quantum computers pose a significant threat to traditional cryptographic algorithms. Their ability to solve complex mathematical problems efficiently can break widely-used encryption methods like RSA and ECC.

Devices with 10~15 years life cycle need PQC Today



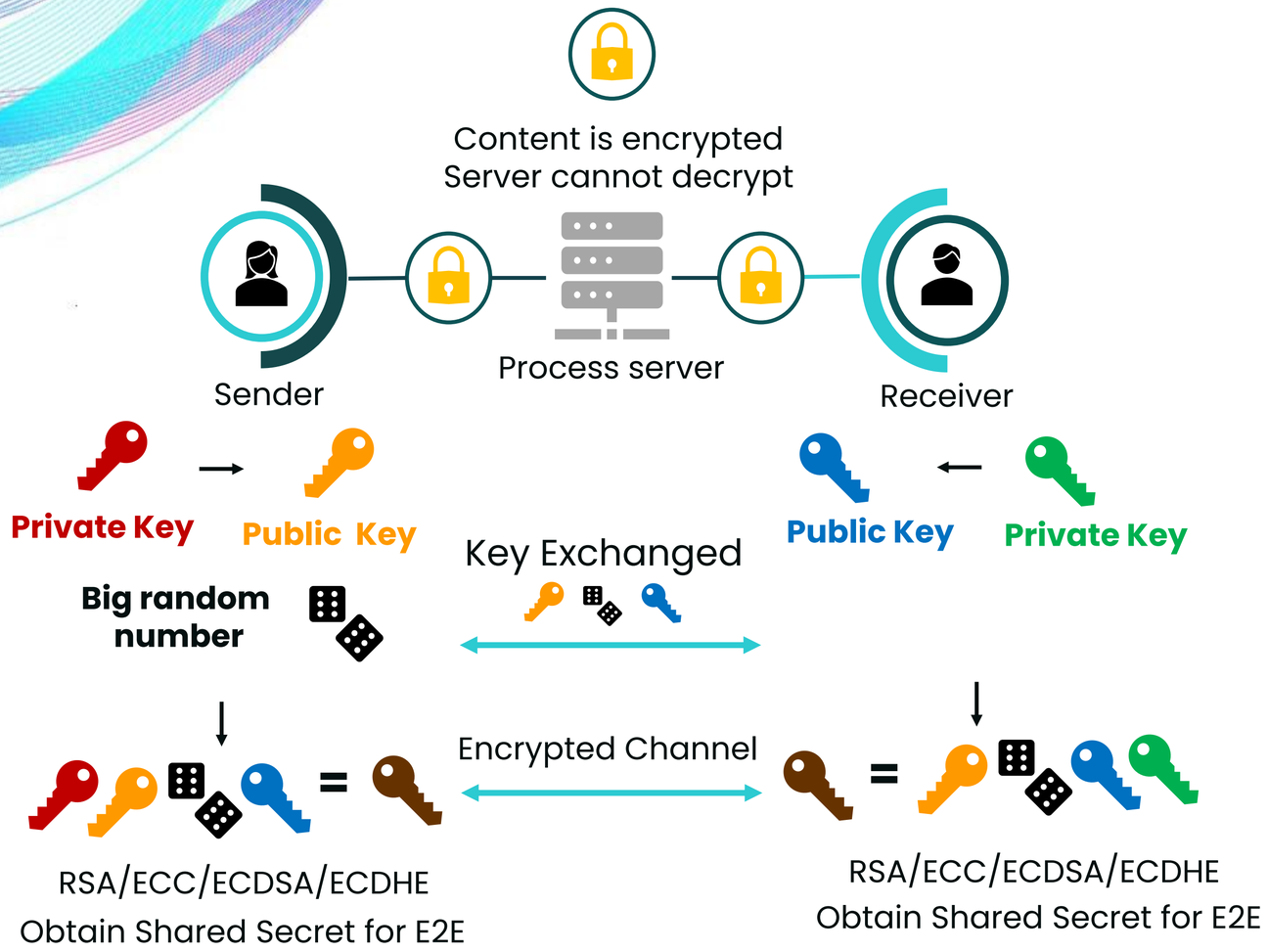
🔑 PQC Algorithms



Post-Quantum Cryptography involves developing algorithms resistant to quantum attacks. Key algorithms include lattice-based, hash-based, and code-based cryptography.

- 🔒 **Lattice-based cryptography**
- #️⃣ **Hash-based cryptography**
- 🔐 **Code-based cryptography**

Internet Security PQC Threat

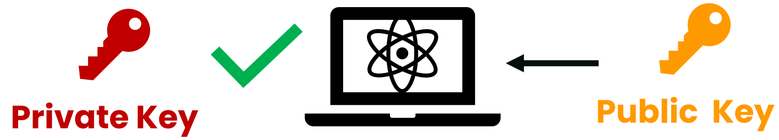


Traditional Computer

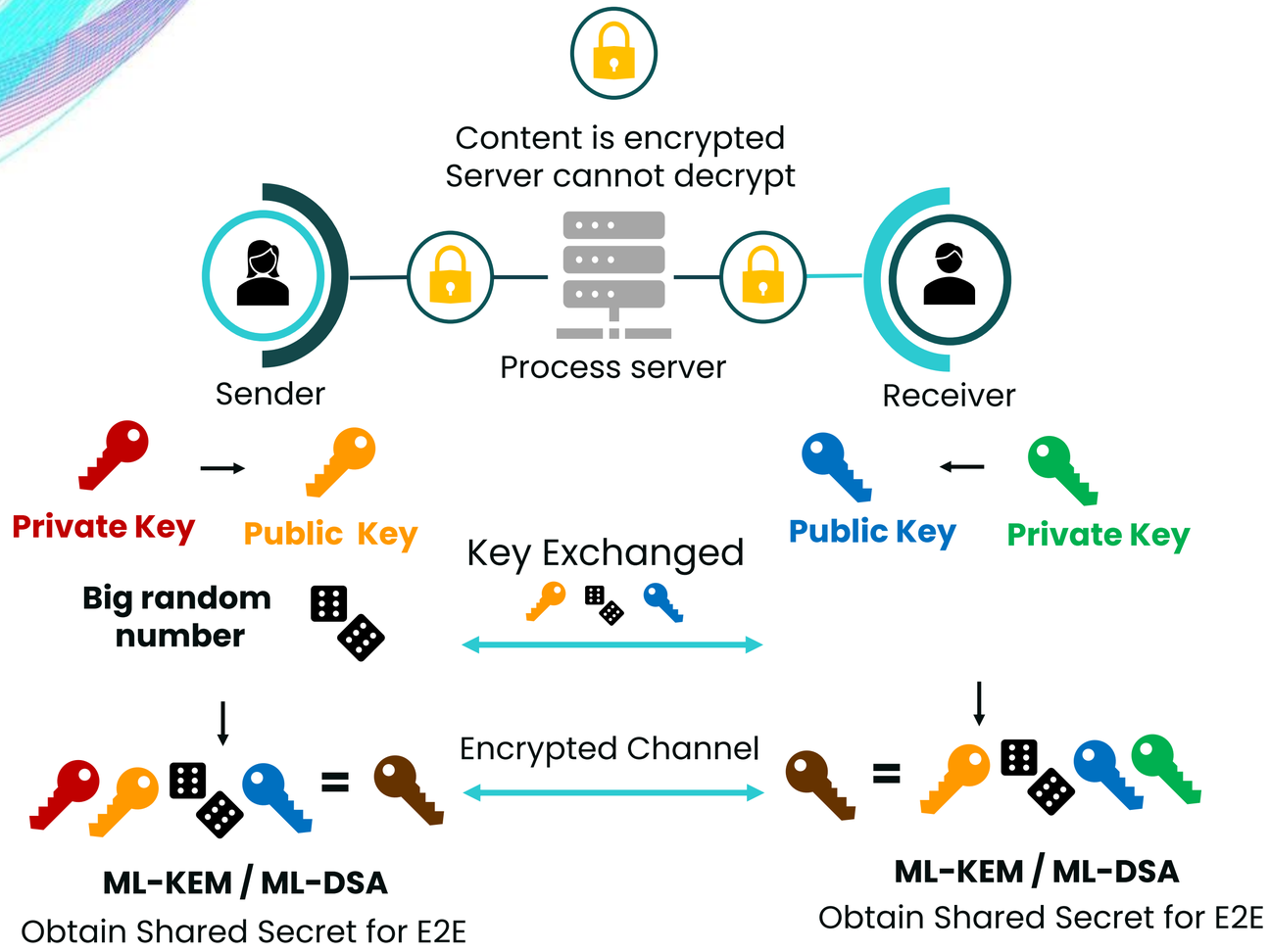
Too much time and process calculation required to “compute back” private key from public key.

Quantum Computer

Quantum computer only needs few thousands Qubits and few hours to “compute back” private key from public key.



Internet Security PQC Solution



NIST
National Institute of Standards and Technology

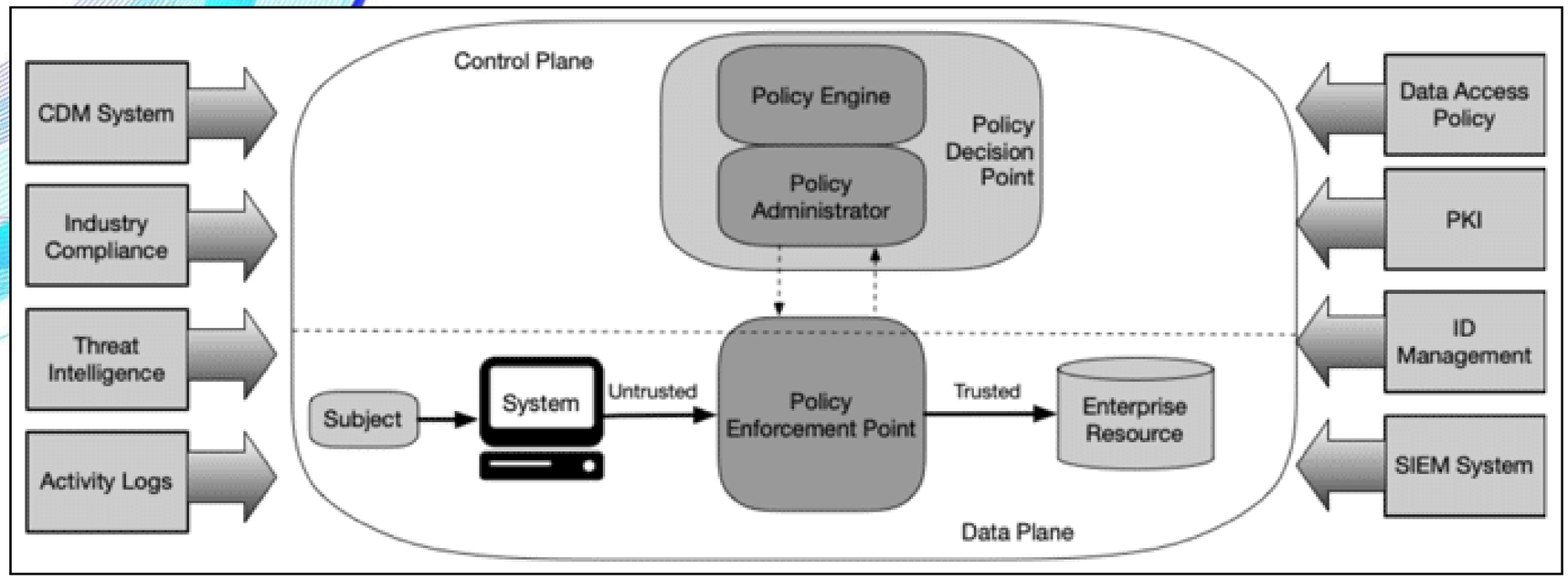
Published August 13, 2024.

Key Encapsulation : FIPS 203
- CRYSTALS-KYBER (ML-KEM)

Digital Signature : FIPS 204, FIPS205
- CRYSTALS-Dilithium (ML-DSA)
- SPHINCS+

- FALCON (in progress)

Zero-Trust Introduction



- Never Trust, Always Verify
- Least Privilege Access
- Secure every connection

- Policy Decision Point (PDP)
- Policy Engine (PE)
- Policy Administrator (PA)
- Policy Enforcement Point (PEP)
- Subject/System
- Resources

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

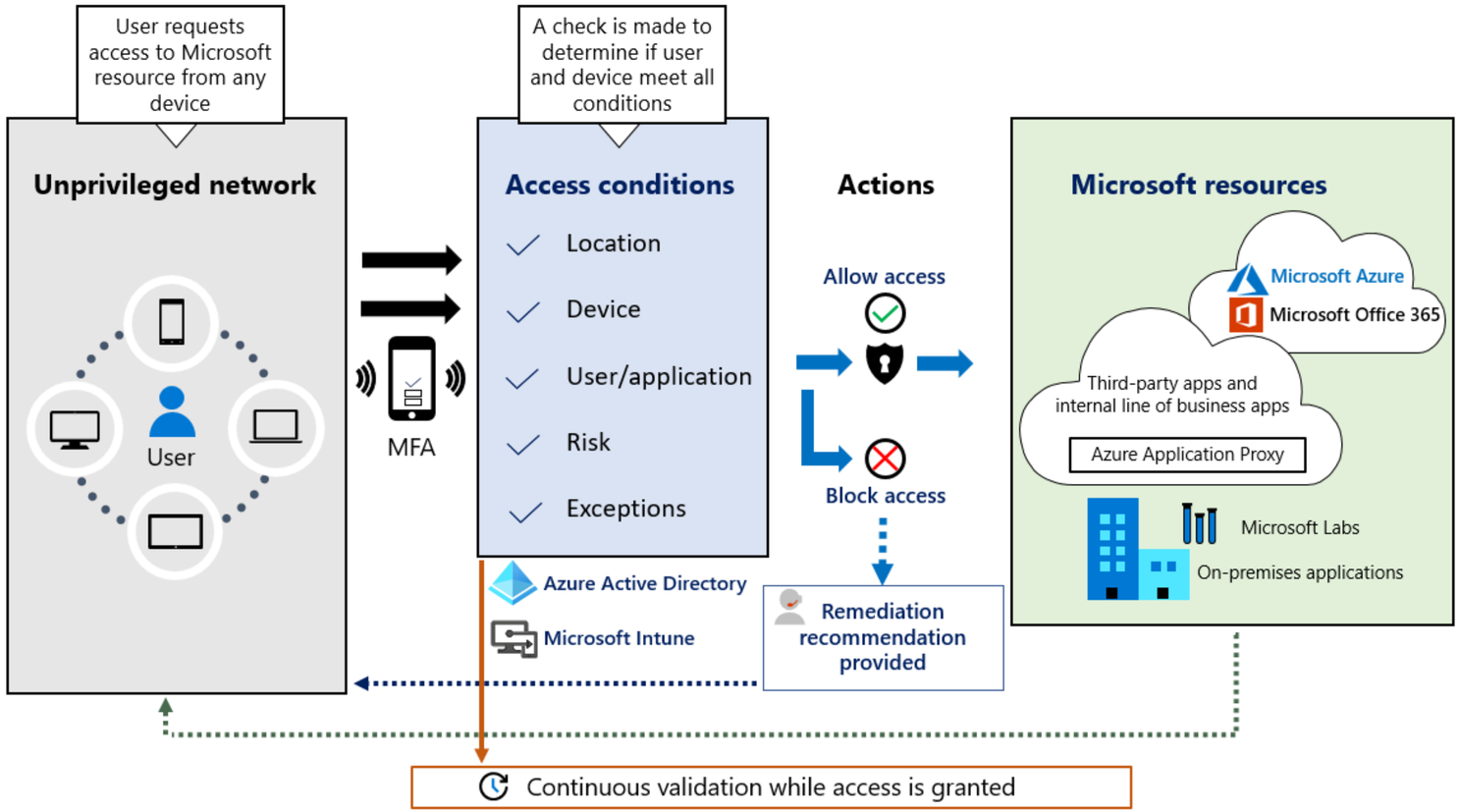
Never Trust Always Verify

Zero Trust Architecture is a security concept based on the principle that organizations should never automatically trust any entity—inside or outside their perimeters.

Instead, they must verify every connection attempt before granting system access.

Requirements and Architecture

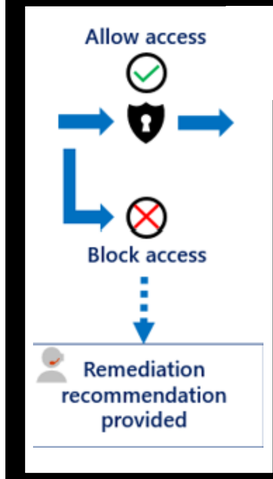
Microsoft



+ PQC secure channels

User login/ID
User Password/Passkey
Device UID

Multiple Factor Authentication (HTOP/TOTP/FIDO)



Admin Tenants / Users System

Continuous validation while access is granted

Additional Continuous Challenge

Source Microsoft : https://www.microsoft.com/insidetrack/blog/implementing-a-zero-trust-security-model-at-microsoft/

CYBERSEC 2025
臺灣資安大會

Generating Keys with Physically Unclonable Function

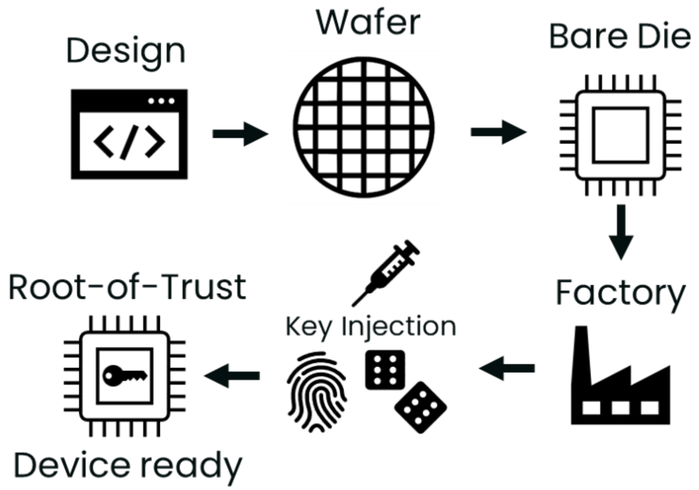
Self-Generating Root-of-Trust

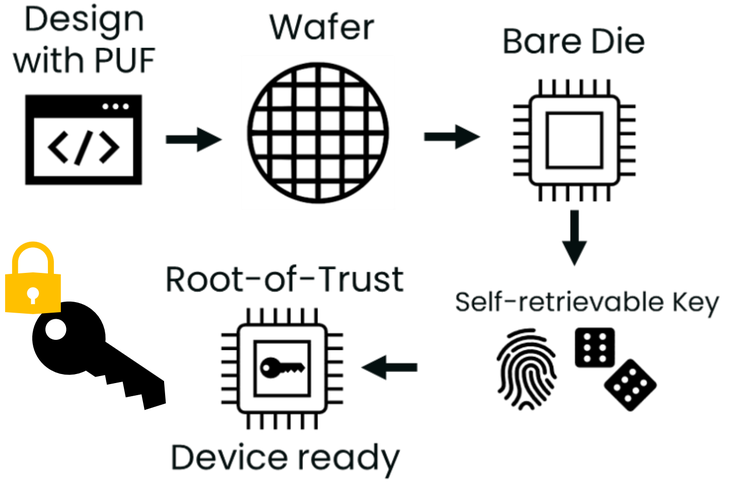
🔮 Principle of PUF : Fingerprint/DNA for Hardware

True randomness comes from nanoscale variation during chips fabrication

PUF stands for **Physically Unclonable Function**.
It acts like a fingerprint for hardware, unique to each device by leveraging nanoscale manufacturing variations to self-generated unique identifiers, secrets and random numbers, the foundation of modern and post-quantum cryptography.

- 🛡️ **Reduce Threats from Untrusted Manufacturer**
- ⛔ **Avoid Known Secrets Injection**
- 🎲 **Truely Random and Unpredictable**





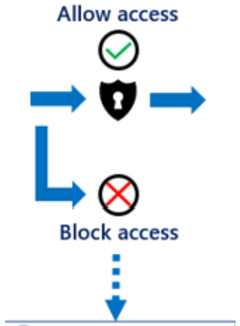
Traditional PUF Usage : Rely on a single root

User login/ID
User Password/Passkey
Device UID

TRNG +KDF

Multiple Factor Authentication
(HTOP/TOTP/FIDO)

TRNG+KDF



Admin Tenants / Users System

TRNG+KDF

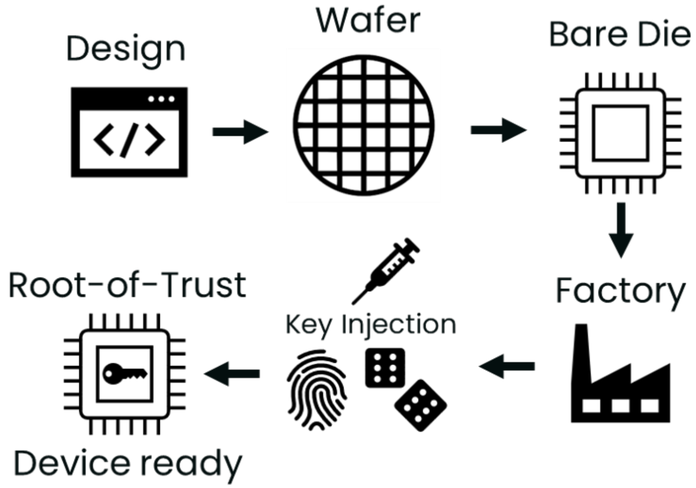
Continuous validation while access is granted

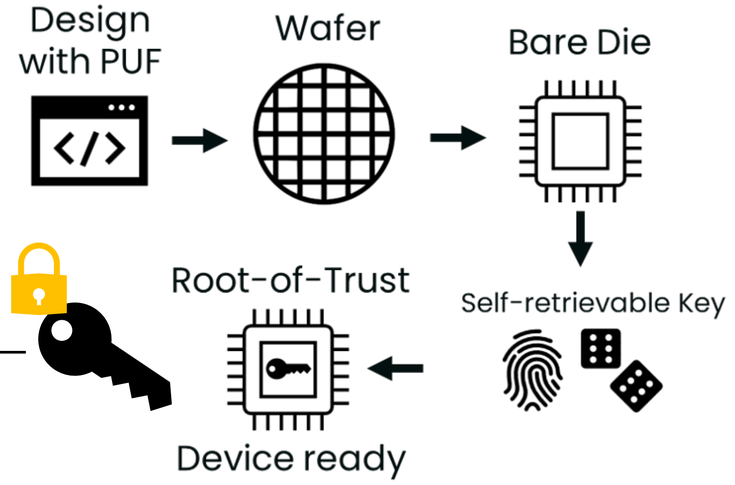
Continuous Challenge

TRNG+KDF

PQC Seeds & Keys

TRNG+KDF





CYBERSEC 2025
臺灣資安大會

IIST

IIST Inc.
Introducing

Dynamic PUF Root-of-Trust

Self-Generating Multiple Root-of-Trust

IIST PUF Technology: Dynamic PUF root-of-Trust

User login/ID
User Password/Passkey
Device UID

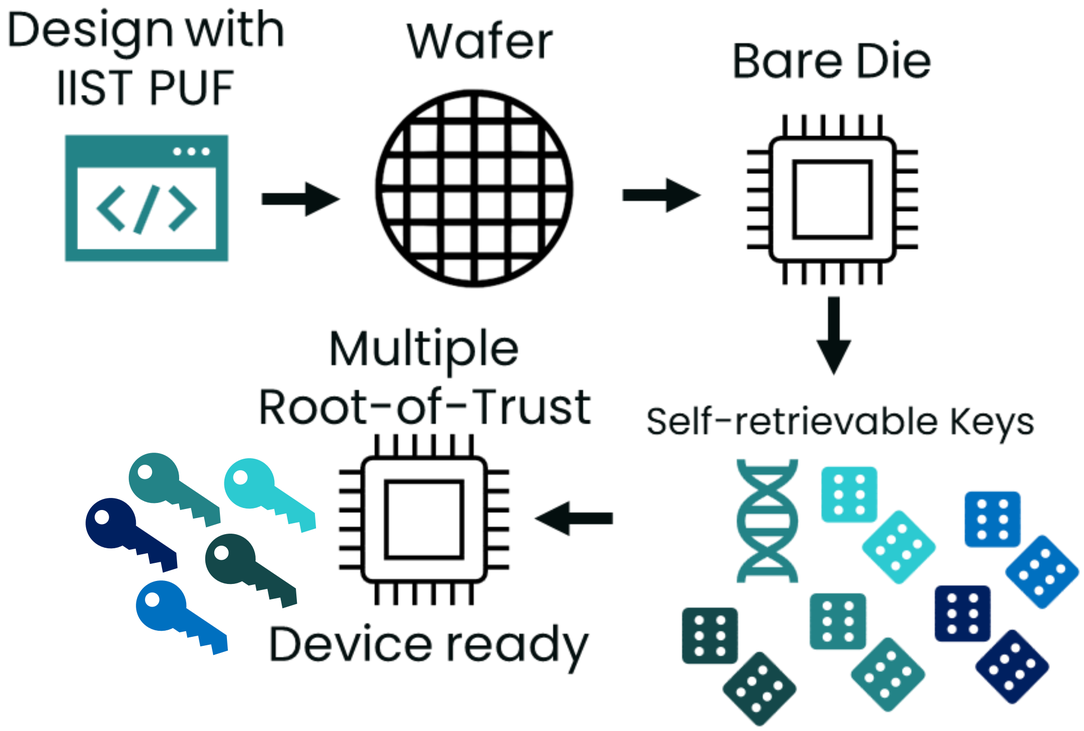
Multiple Factor Authentication
(HTOP/TOTP/FIDO)

Admin Tenants / Users System

Continuous validation while access is granted

Continuous Challenge

PQC Seeds & Keys



IIST PUF Technology: Dynamic PUF root-of-Trust

IIST

User login/ID
User Password/Passkey
Device UID

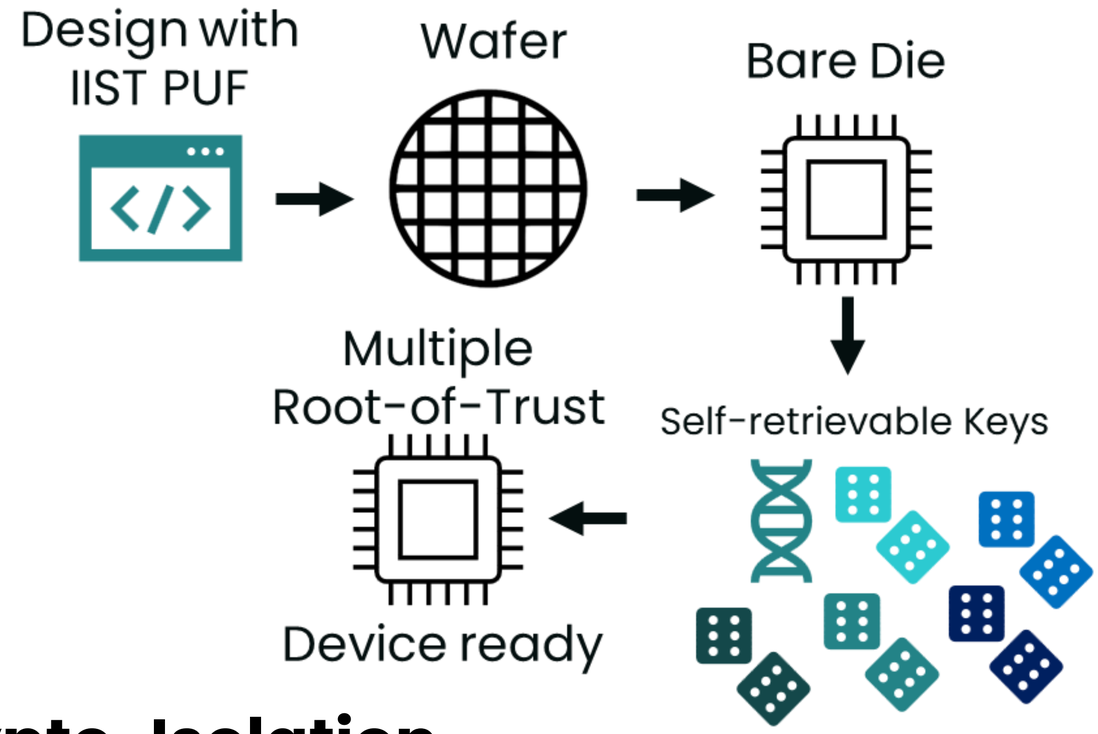
Multiple Factor Authentication
(HTOP/TOTP/FIDO)

Admin Tenants / Users System

Continuous validation while access is granted

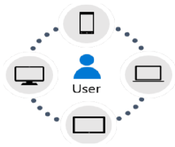
Continuous Challenge

PQC Seeds & Keys



Crypto-Isolation
True Randomness
Power-Independent

IIST PUF Technology: Dynamic PUF root-of-Trust



User login/ID
User Password/Passkey
Device UID

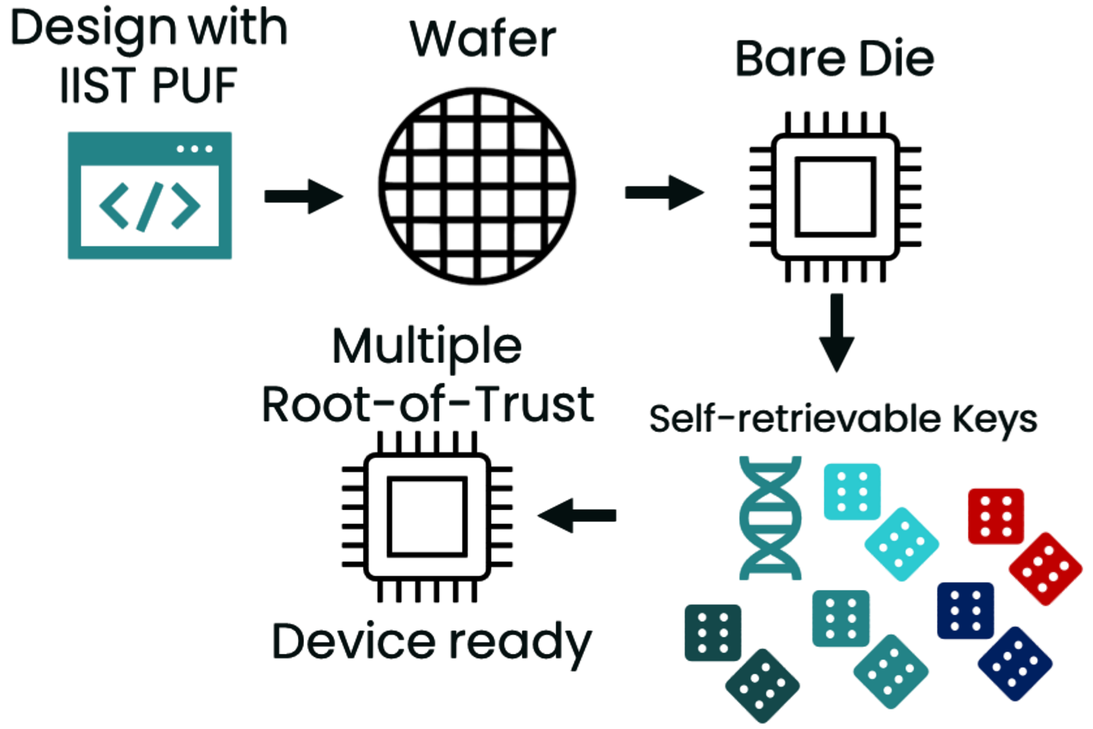
Multiple Factor Authentication
(HTOP/TOTP/FIDO)

Admin Tenants / Users System

Continuous validation while access is granted

Continuous Challenge

PQC Seeds & Keys



Renewable, when necessary, without affecting other roots

IIST PUF Technology: Typical Embedded System Usage

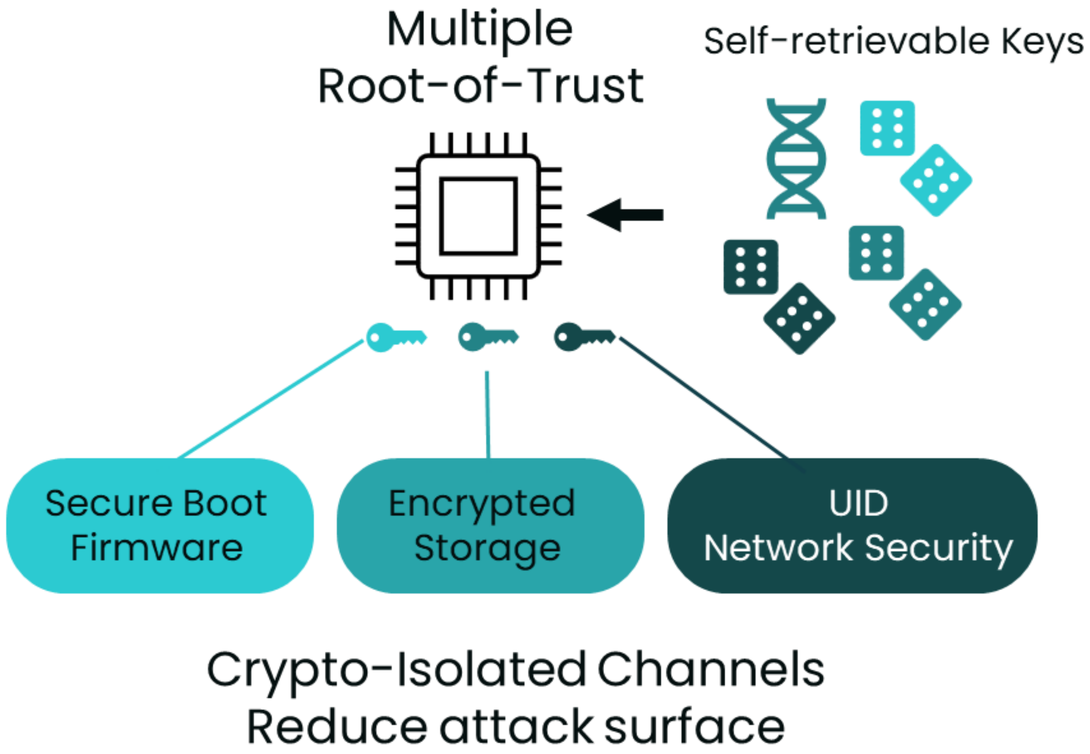
Design a PUF-based root-of-trust for every application and device cycle

Ideal for secure key storage and device authentication. Ensures each device has a unique identity, crucial for IoT and zero-trust environments. Supports crypto isolation, allowing each application to have its own dedicated root of trust with innovative stabilization mechanism for harsh environment such as aerospace or automotive.

🗃️ **Not limited to a single usage**

✅ **Compatible with all technology process nodes**

💪 **Designed for robustness in harsh environment**



CYBERSEC 2025
臺灣資安大會

IIST

IIST PUF-based

Products & Services

Flexible, Versatile, Scalable Solutions

IIST

Authentication challenges in IoT devices create vulnerabilities that cascade through security modules, IC fabrication, and semiconductor design.

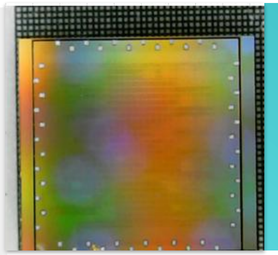
Our innovative hardware solutions, driven by patented dynamic PUF technology, address these issues at the source, delivering scalable and flexible security for the connected world.

Products & Services

Silicon IP

- ✓Silicon Anchor Secure PUF (**SASpuf**)
- ✓NIST CAVP Algorithms with SCA

Submit request for detailed Algorithms list

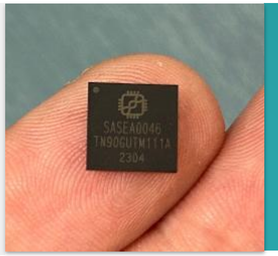


Semiconductor Security Design

Packaged IC

- ✓Silicon Anchor Secure Engine (**SASe**)
- ✓Silicon Anchor Secure Processor (**SASp**)

Submit request for customization



Security IC Chip Production

Modules & USB Keys

- ✓**SASe Module 1** (2024 edition)
- ✓**SASe USB Key 1** (2024 edition)

Submit request for customization & roadmap

Security Modules Integration

Integration Support

- ✓Security products integration
- ✓Field application assistance

Submit request for supports and quotation

System Integration IoT

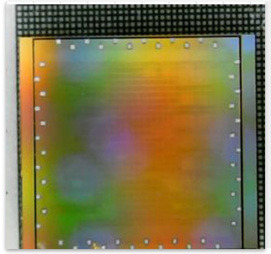
AIoT&Hardware SECURITY ZONE

IIST

Authentication challenges in IoT devices create vulnerabilities that cascade through security modules, IC fabrication, and semiconductor design.

Our innovative hardware solutions, driven by patented dynamic PUF technology, address these issues at the source, delivering scalable and flexible security for the connected world.

Products & Services

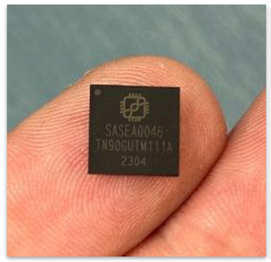


- ✓ Inter-Hamming Distance 50% (+/-) 1%
- ✓ Intra-Hamming Distance 50% (+/-) 1%
- ✓ Entropy Source SP800-90B
- ✓ TRNG SP800-22

NIST

Silicon IP

Semiconductor Security Design



- ✓ HTOL/LTOL 125°C 1,000 hours
- ✓ 3V3 Single Supply
- ✓ UART/SPI
- ✓ SESIP 1 Security Certification
- ✓ SESIP 2 : On-Going

Global Platform® SESIP

Packaged IC

Security IC Chip Production

- ✓ UART/SPI/I2C
- ✓ Programmable Module
- ✓ TLS 1.2/TLS 1.3/FIDO2

Modules & USB Keys

Security Modules Integration

- ✓ Water-Resistant
- ✓ Touch-pad
- ✓ Low-Cost
- ✓ FIDO2 Certified

fido CERTIFIED FIDO2

Integration Support

System Integration IoT

AIoT&Hardware SECURITY ZONE

Integration & Applications

Security from chip to cloud applications
Zero-Trust Architectures
Post-Quantum Ready

IIST

AIoT&Hardware SECURITY ZONE

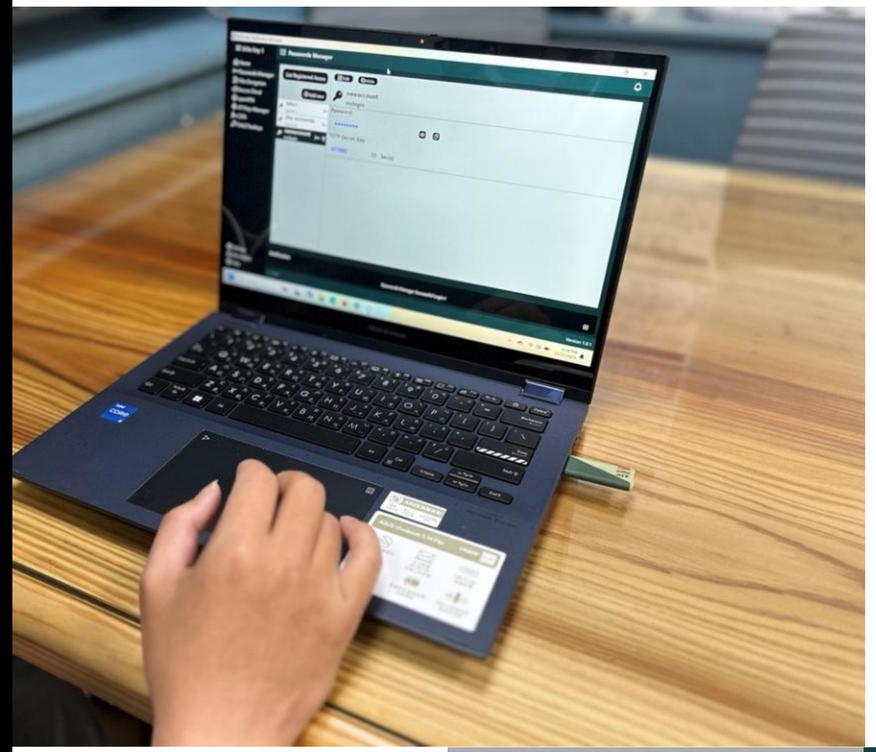
Securing Your Digital World.

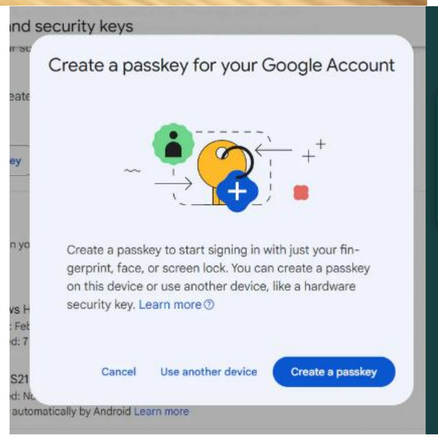
Authenticate

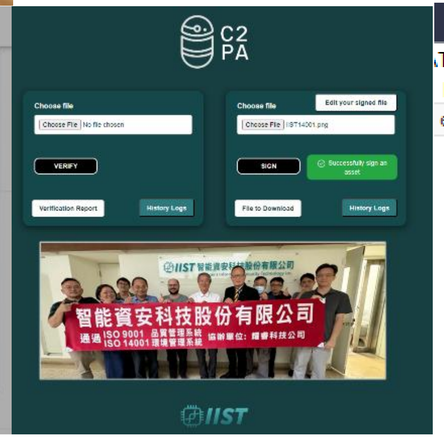
Sign

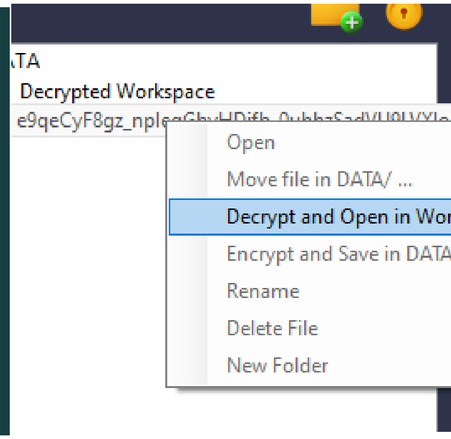
Encrypt

Experience unmatched security with our PUF-powered USB key. Combining FIDO2 authentication, C2PA digital signatures, and data encryption, it delivers dynamic, hardware-based protection for access, integrity, and confidentiality. Secure your digital world with confidence.









IIST

AIoT&Hardware SECURITY ZONE

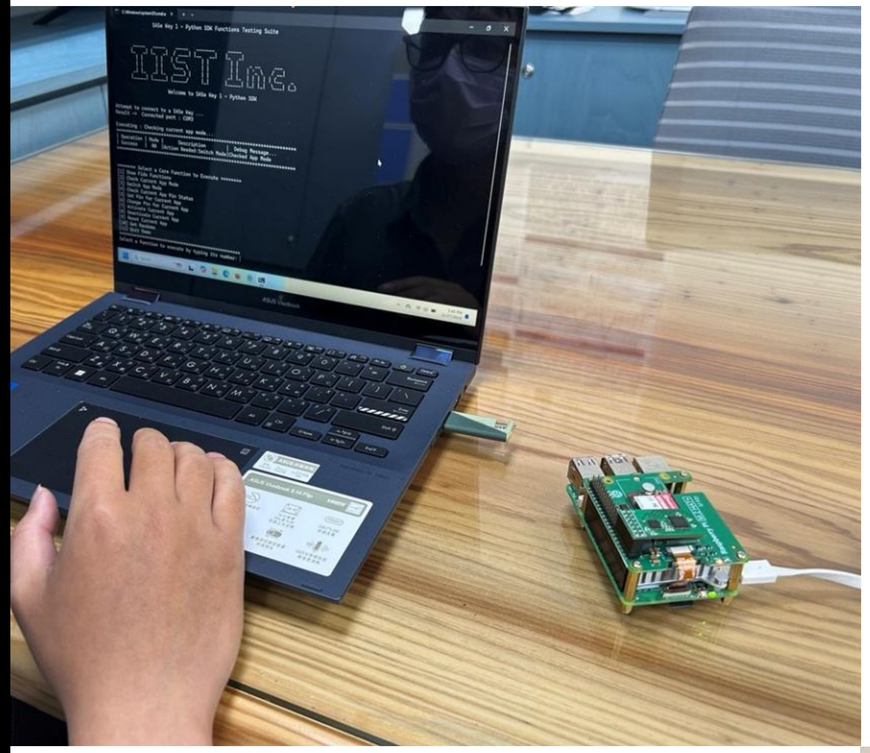
Empowering OEMs and Enterprises with Secure Infrastructures

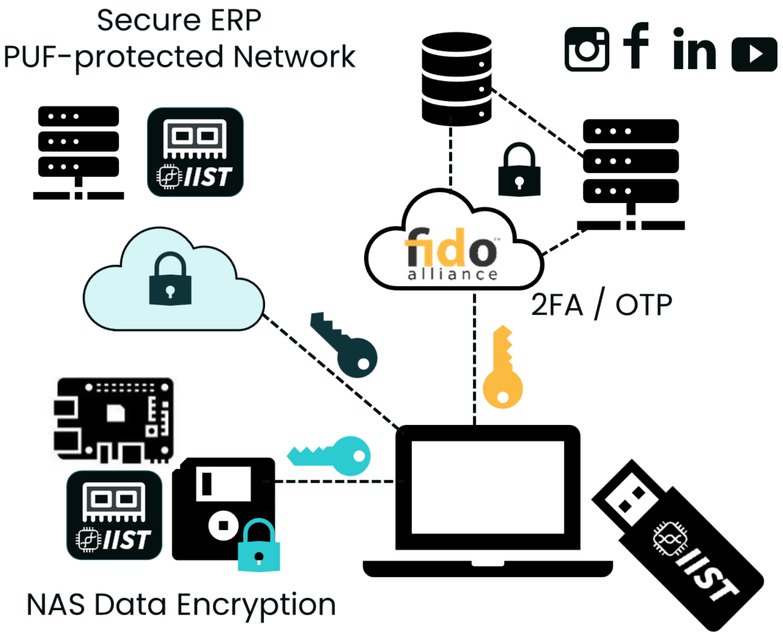
Authenticate

Secure Channels

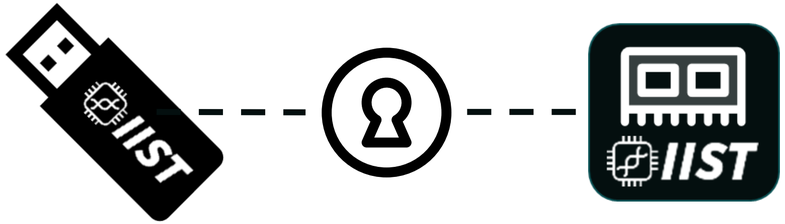
Encrypt

From USB keys to PUF-enabled modules in servers, routers, gateways, and NAS, our solution delivers dynamic cryptographic security for OEMs and enterprises. Simplify secure network administration while protecting your infrastructure with next-generation, hardware-rooted security..



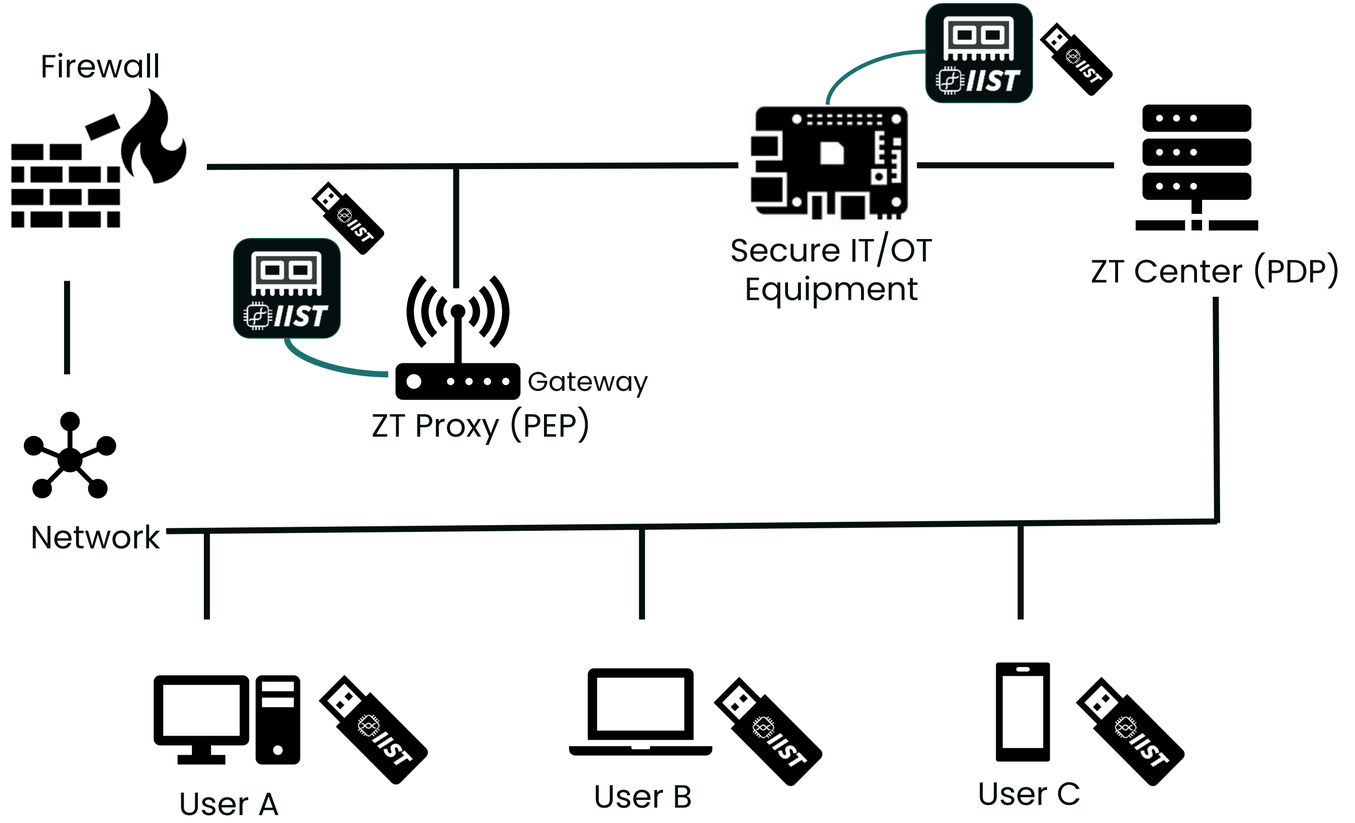


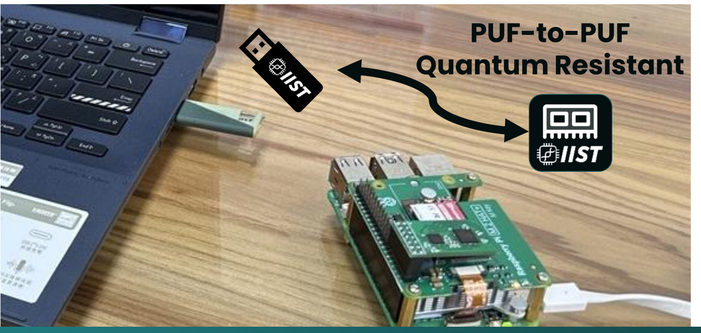
PUF-to-PUF/VPN Secure Channel



AIoT & Hardware SECURITY ZONE

ENHANCING EXISTING ZTA NETWORK WITH PUF HARDWARE





PUF USB Key
Custom ZTPUF

PUF Module
Custom ZTPUF

PUF USB Key alternative

ZERO-TRUST TECHNOLOGY

Zero-Trust PUF

End-To-End ZT Secure Infrastructure

With ZTPUF, enterprises gain the best of both worlds: ZTA-powered network and software management combined with PUF-driven, hardware-bound security. Whether for routers, NAS, gateways, or laptops, our PUF-enabled solutions elevate zero-trust architecture with unmatched credential security and encryption.

NIST SP. 800-207

Augment ZTA with PUF keys and modules

Tailored solutions for Flexible Deployment

PUF technology quantum-resistant

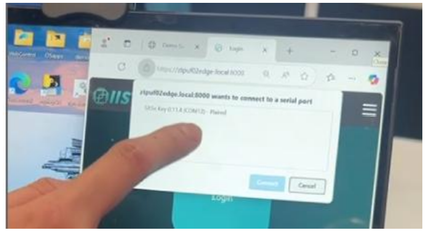
A complete set for total ZTA solution

Endpoint Key

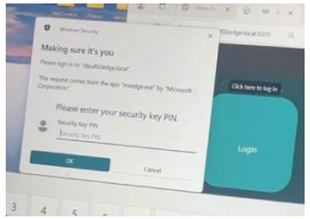
ZTA PUF

Connection

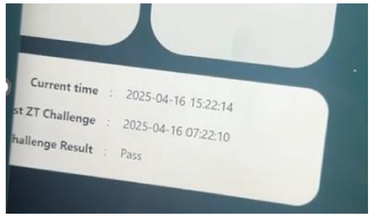
Embedded Module



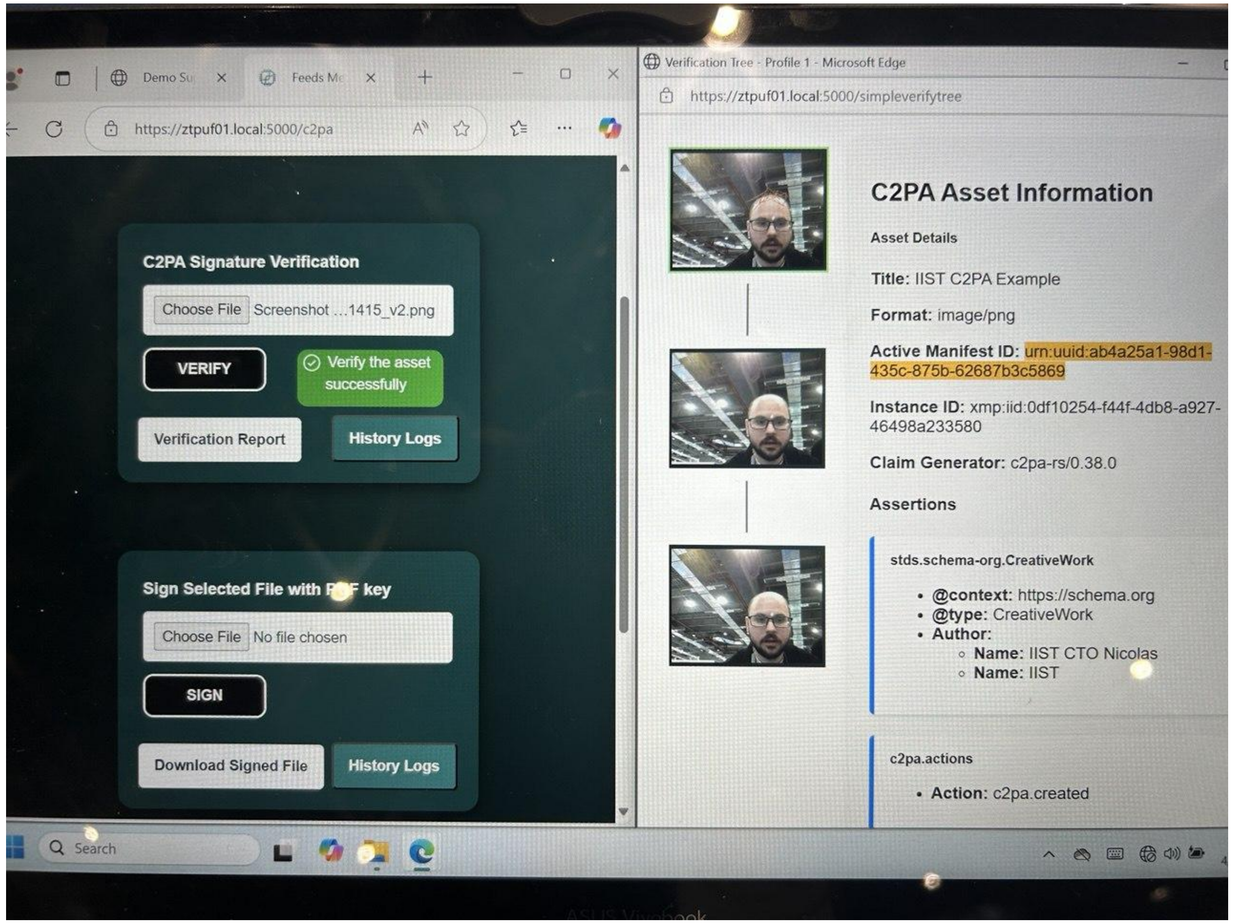
Device ID



fido CERTIFIED FIDO2

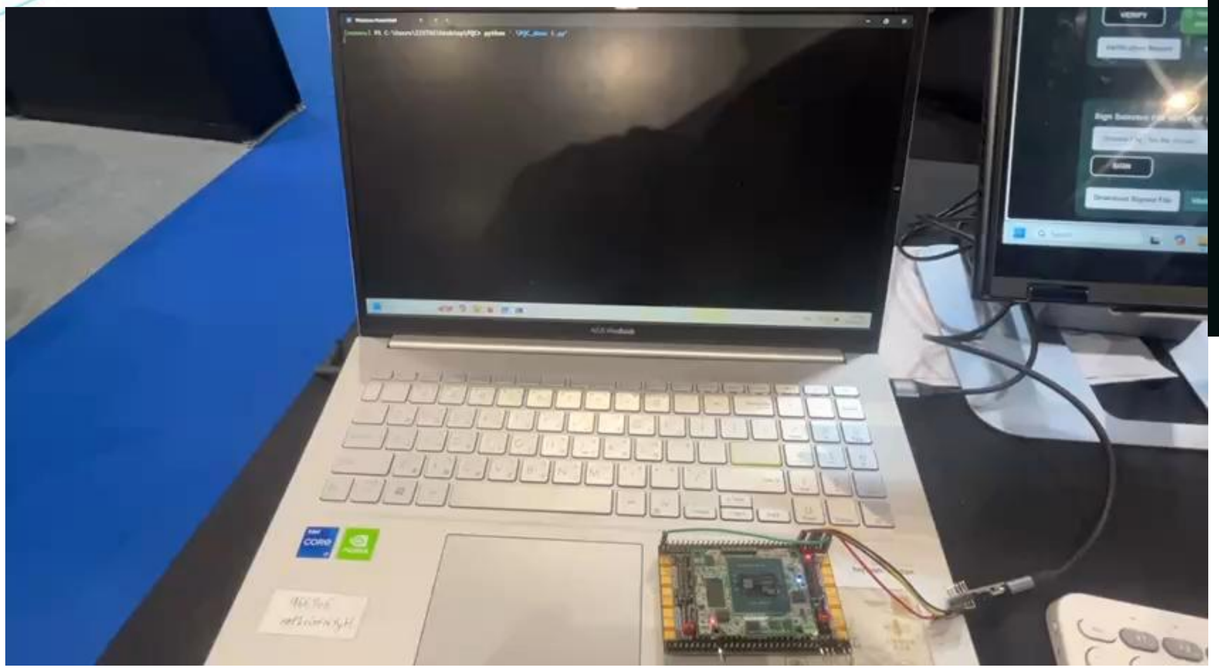


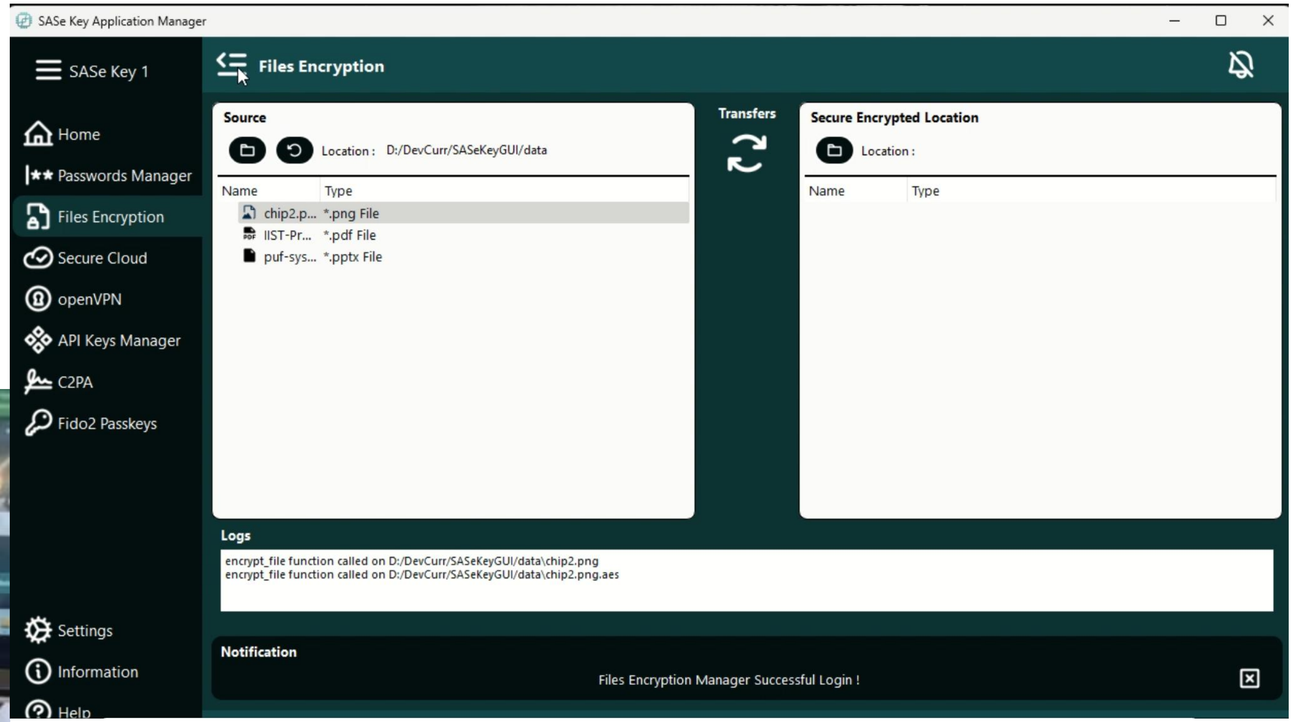
Serial Port Challenge



C2PA Signature

PQC
FIPS 203/204





BUILD YOUR OWN SOFTWARE

WITH OUR API AND SDK

CYBERSEC 2025 臺灣資安大會 | 4/15-4/17 臺北南港展覽二館

WELCOMING INNOVATION AND COLLABORATION

LET'S SHAPE THE FUTURE TOGETHER

Stay Connected With Us

service@iist.com.tw

https://www.iist-site.com

No. 47 Park Avenue 2nd Road Hsinchu City 300091, Taiwan

TEAM
CYBERSECURITY