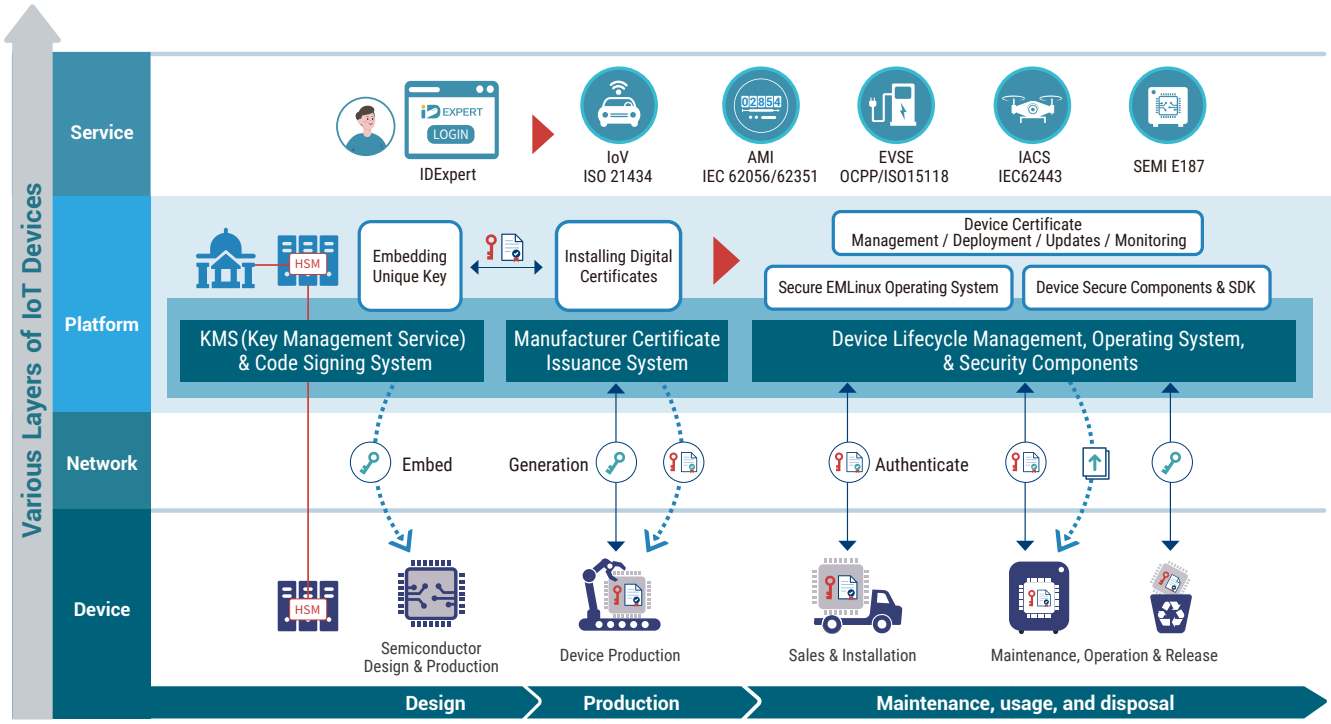
CHANGING

Digital Trust through PKI Enables Infinite IoT Potential

CHANGING IoT Security Solution

CHANGING IoT Security Solution

- Ensure IoT device security throughout their lifecycle with key and certificate management, Zero Trust Architecture & data encryption.
- Utilize PKI technology to integrate machine identity management into a zero trust network architecture.
- Verify device legitimacy to prevent software platform tampering and unauthorized firmware updates.
- Collaborate with multi-domain manufacturers, combining software & hardware to meet international cybersecurity standards for IoT devices.



Systems

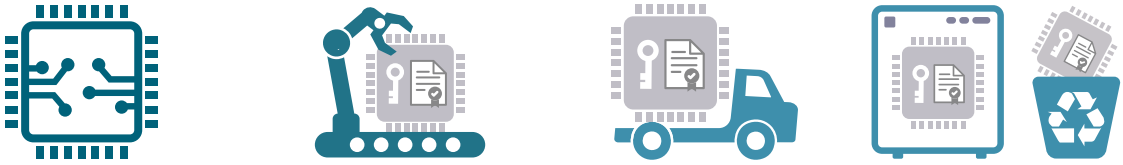
- KMS Key Management and Code Signing System.
- Manufacturer Certificate Issuance System.
- Device Lifecycle Management System.
- Secure Embedded Linux Operating System：10-year maintenance version.
- Device Security Chips and Security Service SDK.
  - Intel x86 architecture TPM - ARM architecture TrustZone or secure chips.
- TrustEnd Hardware Authenticator：various certification carriers, integrated identity authentication services.

Services

- Design and related IP for RoT (Root of Trust).
- Customization of MCU Secure Firmware.
- Chip certificate / firmware , programming and verification.
- Provision of Matter DAC certificates.

IoT security, complete lifecycle protection

Expanding application in device certification across various industries including semiconductor, smart manufacturing, smart cities, IoV, and smart homes, ensuring comprehensive protection from chips to device applications, highlighting the importance of digital trust in IoT.



Semiconductor design &production | Device manufacturing | Sales and installation | Maintenance and operations

Design | Production | Maintenance, usage, and disposal

Device Design Stage

Hardware Root of Trust Design

The Root of Trust (RoT) establishes a unique, immutable, and unclonable identity for devices with secure boot mechanisms in IoT, ensuring robust IoT security.

- For IoT device manufacturers：TrustM / Linux TPM secure module can be adopted.
- For IC design companies：MCU Trust Zone + PUF IP.

Secure Boot and Firmware Updates

Utilizing a hardware Root of Trust with a secure chip allows for device firmware integrity checks. This ensures Secure Boot compliance by automatically verifying firmware integrity at startup. This process enhances device security and reliability by preventing unauthorized modifications. Encrypted and signed secure storage devices further safeguard confidentiality and integrity.

Device Certification and Secure Channels

Utilizing device certificates for mutual authentication establishes encrypted secure channels between devices. This ensures data transmission confidentiality, integrity, and reliability, meeting international standards. Data signing guarantees data integrity and non-repudiation during data transmission.

Device Production Stage

Key Management Service (KMS)

- Generating and storing key pairs required by the KMS system, generating Certificate Signing Request (CSR), and importing certificates issued by Certificate Authorities (CA).
- Private keys can be stored in Hardware Security Modules (HSMs) to protect keys throughout their lifecycle, accelerating signing, verification, and encryption processes efficiently.

Code Signing

- Offering Code Signing services where developers can digitally sign programs, executables, and firmware using code signing certificates. Users can verify the authenticity and integrity of code to prevent tampering.

Manufacturer Production Certificate Issuance

- Providing manufacturers with the ability to establish single or multi-tier Public Key Infrastructure (PKI) to produce, sign, and manage digital certificates required for manufacturing.

IC Chip Secure Programming

- Implementing secure measures during IC programming processes, including key protection, firmware signing, and certificate issuance to ensure IC security, thereby enhancing trustworthiness in subsequent device manufacturing.
- IC programming methods：
  1. Manufacturers establish their own programming devices and systems.
  2. Collaborate with compliant programming facilities, allowing manufacturers to out source programming processes.

Device Maintenance, Operation, and Disposal Stage

Applicable Device Lifecycle Management System

Device Certificate Lifecycle Management

- Using PKI certificates tied to unique IDs for secure lifecycle management from manufacturing to disposal, ensuring identity verification and security at each stage.
- Centralized device identity management allows clear monitoring and easy bulk certificate revocation, ensuring efficient management in incidents or mass device disposal.

Secure Deployment of Device Certificates

- Automates registration, updates, and configuration of device identities using IoT-specific workflows (EST, CMPv2, SCEP, etc.), ensuring unique and secure identities for effective large-scale device management.

Device OTA (Over-The-Air) Security Updates

- Pushing new software/system updates to devices over the network for automatic installation, facilitating quick updates and reducing maintenance costs.

Device Certificate Monitoring

- Status Monitoring：real-time monitoring of device operational status including health, connectivity, and uptime.
- Event Monitoring：detecting and logging all device-related events such as alarms, errors, faults, and accesses for immediate response and necessary actions.
- Proactive Monitoring：actively monitoring devices rather than passively waiting for alarms or events to occur.

Recognized for Technical Expertise, Continuously Pioneering New Service Innovations.

Government
Zero Trust Network
Identity Authentication

Government
Zero Trust Architecture
Device Authentication

- Certified in zero trust network identity and device authentication by the Cybersecurity Agency.
- Security certification solutions accredited with FIDO and OATH, using multiple authentication mechanisms.
- ISO 27001 certified, promoting comprehensive information security.

Authorized distributor

CHANGING Information Technology Inc.
www.changingtec.com
+886-3-563-0688
2F, 48 Park Ave.2, Hsinchu Science Park,
Hsinchu 30844, Taiwan