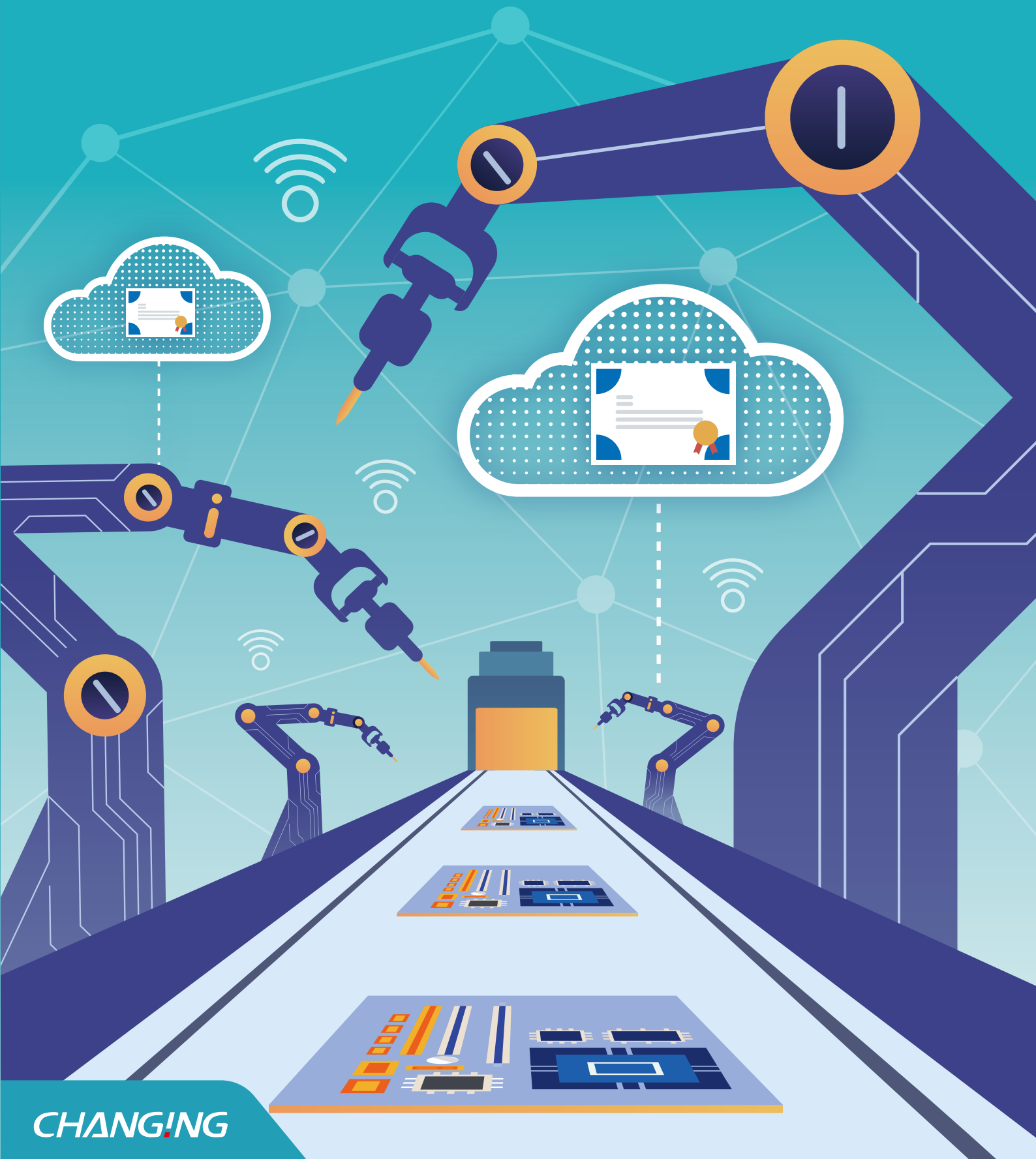
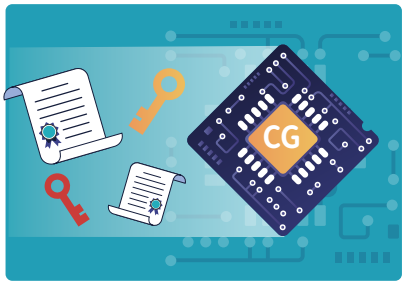
IoT Era
Key Services for Device Security Authentication



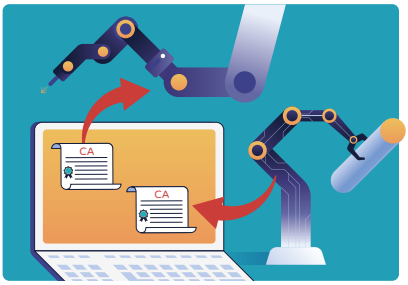
CHANGING

CHANGING IoT Security Solution

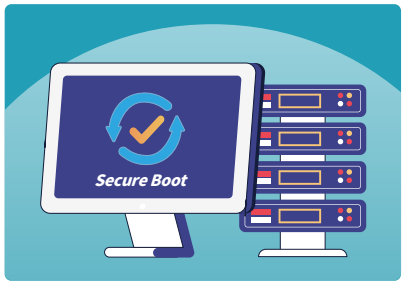
Throughout the device lifecycle, our solution offers diverse security measures, including device key generation and management, certificate management, and IoT security services. It integrates machine identity management into a comprehensive security system, establishing a "zero-trust network architecture" for IoT and supply chains. This addresses blurred network boundaries, verifying device legitimacy, preventing unauthorized software alterations and firmware updates, and ensuring TLS transmission security and data encryption. This ensures secure data transfer, maintaining IoT's convenience while prioritizing safety.



CodeSign Service

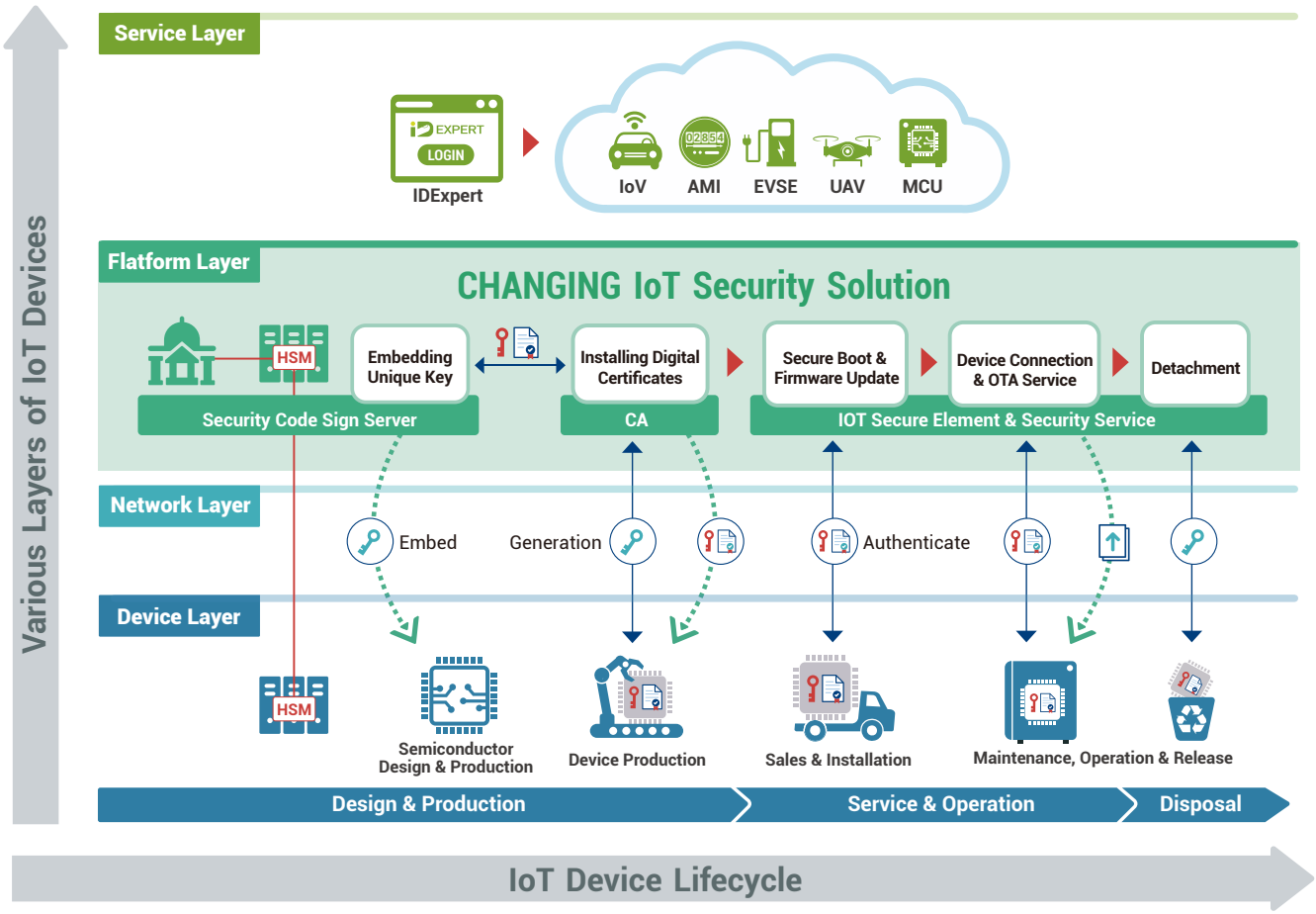


CA Device Certificate Management



IoT Security Services

Architecture Diagram



CodeSign Service

Key Signing and Encryption Control

Operated in conjunction with a Hardware Security Module (HSM), this system involves embedding unique private keys in the secure area of the chip, enabling secure chip encryption, decryption, and digital signature verification capabilities.

- Employing private key signatures ensures the integrity and non-repudiation of sensitive data, guarding against forgery and tampering.
- Utilizing public key verification ensures secure firmware updates and enables safe system initialization.

HSM Cluster Key Management

Smart query of the key list set in Master or Slave Slots within the Cluster, providing information including key status, name, type, activation and deactivation dates. Users can also perform flexible fuzzy searches using key names. Additionally, it supports encryption algorithms such as RSA, ECDSA, DES, 3DES, AES, catering to varying security levels.

HSM Integrated Management

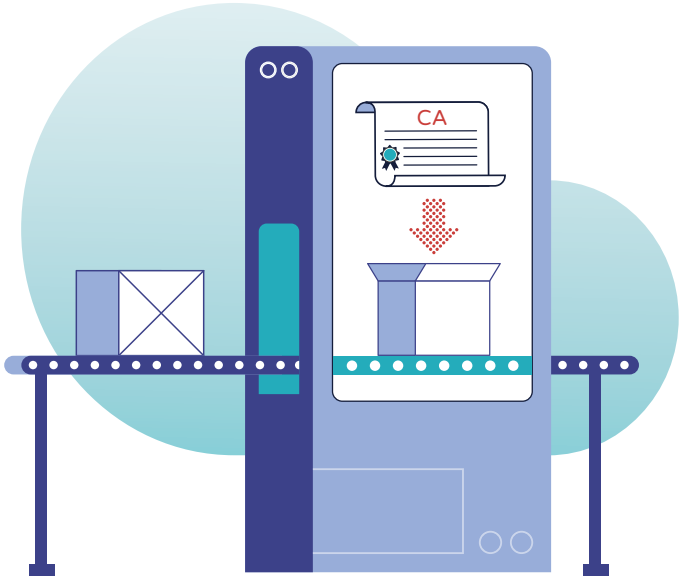
Allows for HSM connection, synchronization, and related operations. Users can input HSM information within the system, including name, brand, IP, slot, etc., facilitating setup and management.

CodeSign Program Code Digital Signing

Digitally sign software or code to enable users to verify the authenticity (source) and integrity of the code, while preventing tampering.

- Supports Code Sign operations for file types like ActiveX, Jar, exe, dll, img, bin, apk, etc.
- Integrates client-side SignTool for firmware Code Sign operations.
- Capable of batch Code Signing or single-file Code Signing uploads.
- Supports third-party CA certificates or self-signed certificates.

CA Device Certificate Management



Apply for device certificates to authenticate the legitimacy of devices.

Utilizing a device's Certificate Management System (Certification Authority) fulfills the certificate loading requirement for device manufacturers prior to IoT device shipment. With unique device IDs and certificates, it ensures the legitimacy of device deployment.

Batch produce certificates through the CA Certificate Center, ensuring streamlined and swift processing.

Register CA with cloud services → Place private keys in HSM for certificate issuance → Batch produce certificates.

Provide APIs to facilitate a smooth and secure device production process.

- Production Workstation API: Receives certificate-related files and loads certificates onto IC chips, simultaneously transmitting certificate data to the certificate production management system.
- QC Workstation API: Verifies the correct writing of certificates.

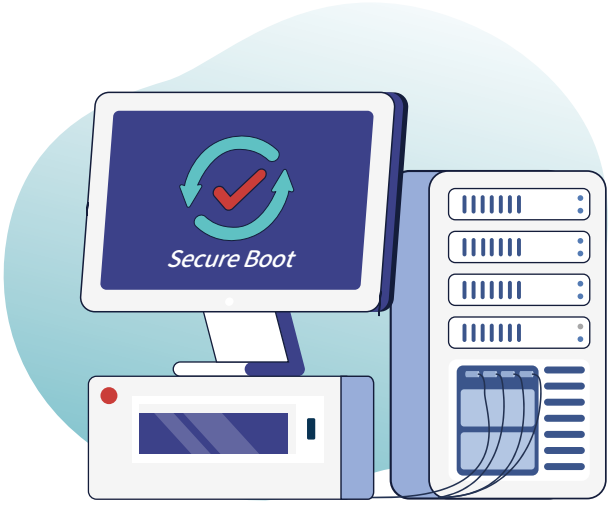
IoT Security Services

Bidirectional Authentication and TLS Secure Channel

Utilize device certificates for mutual authentication, verifying the validity of each other's certificates. Devices establish an encrypted secure channel for data transmission between them using Bluetooth, WiFi, WANGOX, or NBT connections. This ensures data confidentiality, integrity, and reliability in accordance with international standards.

Hardware Security Chip

Featuring the certified Infineon OPTIGA™ TPM and OPTIGA™ Trust M security chips, verified with Common Criteria EAL6+ certification, these chips incorporate independent microprocessors and storage areas. They can achieve physical isolation from device terminal operating systems and application software execution environments, ensuring a high level of security. Their core functions such as secure boot, access control, and storage effectively counteract hacking attacks.

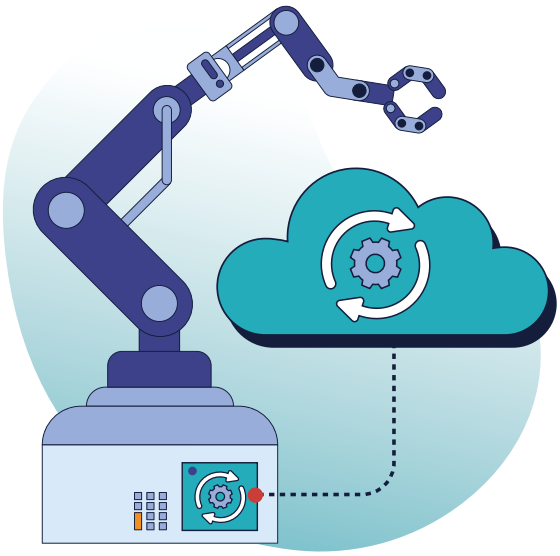


Device Secure Boot

Security chips demonstrate secure protection with a trusted root, offering device firmware integrity checks that meet Secure Boot requirements. During device startup, the firmware is automatically examined for alterations, and the device is allowed to start only if the check is successful. This enhances device security and reliability.

Over-the-Air (OTA) System Upgrades

During the OTA (Over-The-Air) upgrade process, the latest version of software or system is pushed to terminal devices via the internet. In this process, terminal devices don't need to be connected to a computer or use a USB cable. Upon receiving the update package through the network, the terminal devices can automatically complete the upgrade. This approach allows for swift and convenient system or software updates, while also reducing maintenance costs for both end users and service providers.



OTA Ensures Connection Security

The OTA online upgrade service employs a comprehensive security mechanism throughout the process. This includes Transport Layer Security (TLS) mutual authentication for secure interaction, OTA update traffic management and delivery through the Panoramic OTA Server. Every HTTP or MQTT message passing through the OTA server, both incoming and outgoing, undergoes authentication and authorization. Additionally, device firmware can be digitally signed before OTA updates, ensuring it originates from a reliable source and hasn't been tampered with.

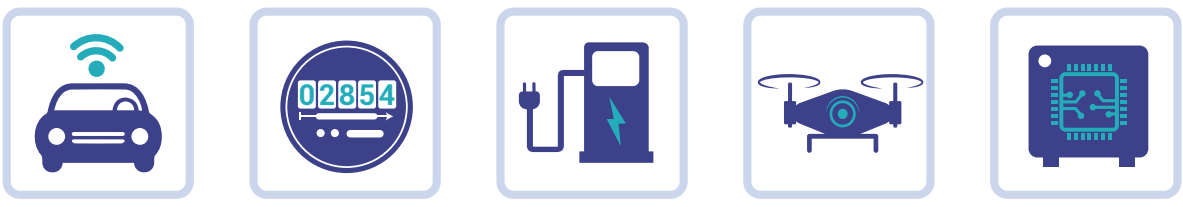
Compliant with International Cybersecurity Standards

Assisting device manufacturers to incorporate cybersecurity compliance into consideration during product design and manufacturing.

- U.S. Federal IoT Cybersecurity Act
- International Industrial Cybersecurity Standard IEC 62443
- European Commission's Proposed Cybersecurity Resilience Act

Diverse Applications

In IoT services, applying Multi-Factor Authentication (MFA) enhances user identity security, preventing unauthorized access and data leaks.



IoV AMI EVSE UAV MCU

Authorized Distributor

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