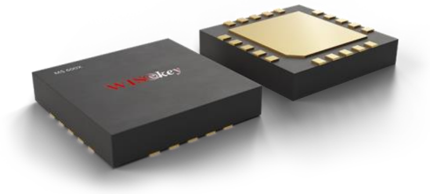
SECURE MICRO-CONTROLLERS & EMBEDDED FIRMWARES

Wisekey Semi-conductor’s division is one of the only 6 semiconductors companies in the world that can develop certified secure micro controllers.

For more than 20 years we have been developing secure chips, secure embedded firmware, and trusted hardware provisioning services, leading to more than 51 families of patents related to secure micro controllers.

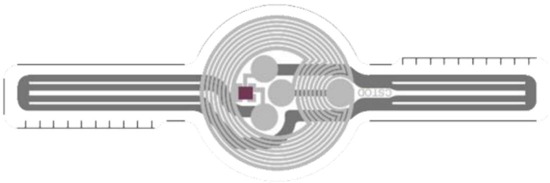
Our chips are compliant with the most demanding certification bodies in the world (Common Criteria EAL5+ & FIPS 140-3) All chips are designed, tested and produced using the highest standards of security, reliability and quality. Operations are run under certified environment (ISO 27001)



DISCOVER OUR COMPREHENSIVE RANGE OF SECURE CHIPS VAULT-IC 155

Secure Element embedded into a unique patented NFC Tag form factor designed for anti-counterfeiting, track & trace, and consumer engagement applications. Compatible with Blockchain & NFT authentication.

Use-Case & References



KEY FEATURES

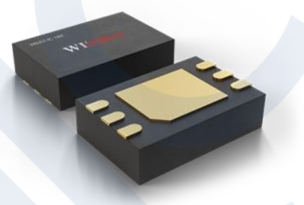
Hardware security level: CC EAL4+
File System size: 1.5KB
Communication: NFC (Iso14443B, NDEF)
Cryptography: ECC up to 303 bits

Typical use: NFC tags for anti-counterfeiting Compatible with blockchain applications (NFT authentication)

VAULT-IC 18X

Secure chip designed to enable Device to Host authentication by contact for anti-counterfeiting applications (Ex: Batteries, Toner Cartdriges…)

Use-Case & References



KEY FEATURES

Hardware security level: CC EAL4+
File System size: 1.5KB
Communication: I2C (Vault-IC 183) / OWI (Vault-IC 186**)**
Cryptography: ECC up to 283 Bits

VAULT-IC 408

Top-Notch security-by-design for IoT devices

Use-Case & References

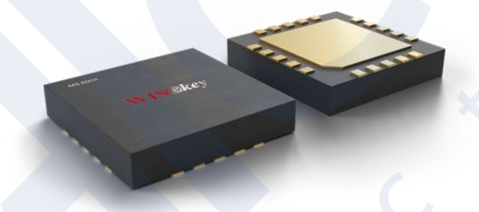
KEY FEATURES

Hardware security level: CC EAL5+
Software Security level: FIPS140.3 CMVP Level 3
File System size: 16 KB
Communication: I2C, SPI, USB, 5 GPIO
Cryptography: ECC (572 bits), AES, DES, 3DES
Digital Sign: DSA/ECDSA [Link to Complete Datasheet] –

MS6001/MS6003

The perfect tamper resistant certified platform to develop sensitive applications running on USB keys

Use-Case & References



KEY FEATURES

Hardware security level: CC EAL5+
Software Security level: 32bit ARM SC300 core
File System size: 1MB Flash/24K RAM
Fully integrated USB interface:
– 48MHZ clock integration
– 8kV ESD protection
– Nano powered real time clock

Complete library & dev guidelines

VAULT-IC 292

Cost effective secure element to enable TLS and secure authentication to cloud and objects.

KEY FEATURES

Hardware security level: CC EAL4+ ready
Software Security level: FIPS140.3 CMVP Level 3
File System size: 2KB (static)
Communication: I2C
Cryptography: ECC (256 bits)

Digital Sign: ECDSA