VaultIC for IoT

Top Security, Easy Integration

VaultIC is a family of **tamper resistant secure chips** with firmware that brings digital security and cryptographic functions to IoT devices, as part of WISeKey's scalable security framework **WISeKeyIoT**. These chips provide configurable cryptographic services for authentication, data confidentiality and integrity check.

VaultIC offers a wide bundle of standard, NIST-recommended cryptographic algorithms (e.g. ECC, RSA, ECDSA, AES, SHA) and associated key lengths.

A certified hardware-based True Random Number Generator complements this set of features. VaultIC also provides on-chip secure data storage for secret keys, certificates and data.

VaultIC comes with a rich software environment including tools for protected boot, secure firmware update for IoT devices and secure communication (SSL/TLS) stacks.

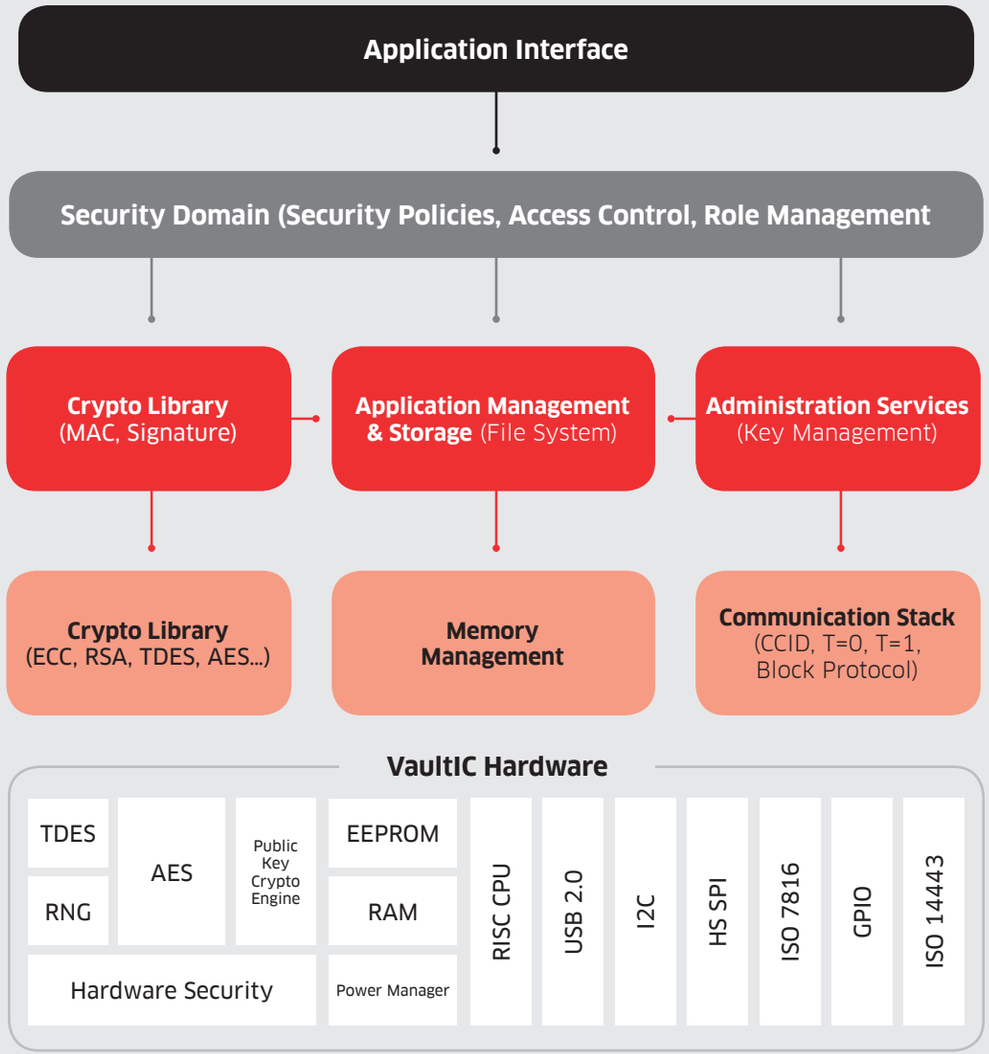
Security
- Security services based on tamper-resistant hardware and embedded software
- Designed to meet C.C. EAL5+ and FIPS 140-2 certifications

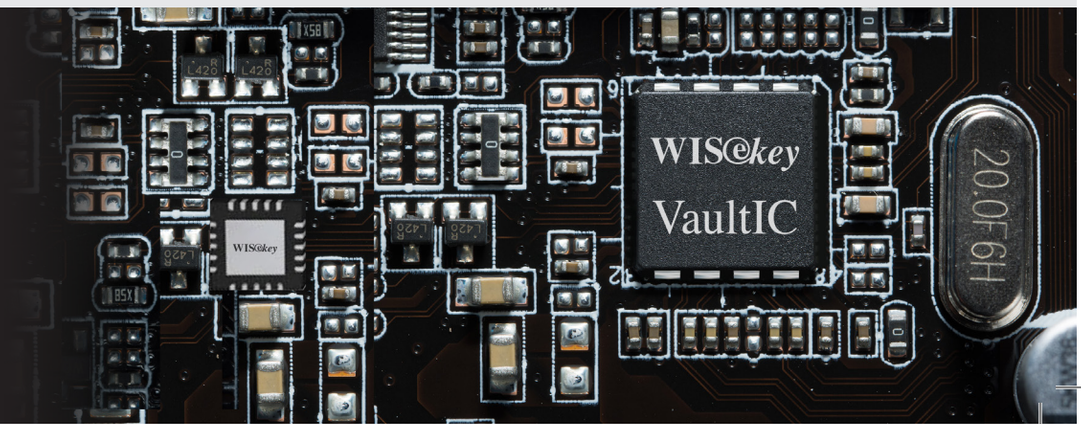
Low power architecture

Secure data storage
- From 1.5 to 112KB

Easy integration
- I²C, SPI, ISO 7816, USB 2.0 full speed interface, USB CCID-compliant, GPIOs
- Industry standard packages
- Software environment: Secure boot, secure update, API...

Internet of Things
- Industry 4.0
- Energy & water
- Smart meters
- Building security, video surveillance cameras...
- Smart Cities (street lighting, waste management...)
- Telehealth, health monitoring...
- Fiscal printers, cash registers...





VaultIC

Implementation Support

The VaultIC starter kit provides a user-friendly hardware and software package for product evaluation and application development.
It includes:

Software

> Getting Started Guide
> Application notes
> VaultIC Manager to personalize the VaultIC File System
> Demonstration application to learn VaultIC features
> Advanced tutorial scripts to accelerate familiarity with VaultIC
> High-level cryptographic libraries for easy system Integration (for Windows, Linux and Mac environments)
> PKCS#11, Windows CSP libraries (refer to EasyPlug)

Hardware

> Product samples
> Evaluation board
> USB-to-SPI/I2C adapter
> USB dongle

Support

> Development support by our technical staff

Supported Standards & Some Key Features

Strong Challenge-Response Authentication
- ISO/IEC 9798-2, FIPS 196, Microsoft Card Minidriver, Global Platform v2.2 SCP02, SCP03 & SCP11

HOTP – One Time Password Generation
- OATH Hash-based OTP algorithm (RFC 4226)

Digital Signature Generation / Verification
- PKCS#1 v2.1 RSASSA-PSS & RSASSA-PKCS1 v1.5
- Raw RSA X.509with no padding
- FIPS 186-2 DSA, ANSI X9.62 ECDSA over GFp and GF2m

Message Authentication Codes (MAC)
- ISO/IEC 9797-1 CBC-MAC/MAC with DES/3DES
- NIST SP 800-38B AES CMAC, NIST SP 800-38E AES-CCM, AES-GMAC
- FIPS 198 HMAC with SHA1 to 512

Data Encryption/Decryption
- DES/3DES-EDE and 3DES-EEE with ECB, CBC, CFB or OFB chaining modes
- NIST SP 800-38D AES-GCM, NIST SP 800-38A AES-CTR D
- PKCS#1 v2.1 RSAES-OAEP, RSAES-PKCS 1 v 1.5
- Raw RSA X509 with no padding

Random Number Generation
- NIST SP 800-90 Deterministic Random Bit Generator using AES-256

Secure File Management
- Static or Dynamic file system,
- Folders can be password protected
- File access rights can be defined to protect user-sensitive data

Secure Communication Channel (with MAC and encryption)
- Global Platform v2.2 (SCP03, SCP11 secure channel using AES)

Key agreement/Key Derivation
- Key agreement ECDHE NIST SP800-56A
- KDF concatenation NIST SP800-56A

Public Key-Pair Generation
- PKCS#1.5 RSA, ANSI X9.31 DSA, ANSI X9.62 ECDSA

Security Certification

VaultIC, the best digital security guaranteed by independent certifications:
> FIPS 140-2 Level 3
> Based on state of the art secure microcontrollers certified to Common Criteria EAL4+/5+
> WebTrust seals for Public Key Infrastructure and Certification Authority root key (annual audit by third party)

Personalization

VaultIC can be initialized with a certificate signed by the International Secure Electronic Transactions Organisation (OISTE) root key.

WISeKey can also perform the full personalization of the VaultIC following the customer's requirements including the chip configuration and file system download.

Product	File System (KB)	Cryptography	Interfaces and Peripherals	Voltage (V)	Temperature Range	Standard Packages
VaultIC182/192	1.5	ECC	I²C	1.62 - 3.3	-40 / +105	DFN6
VaultIC405/405RS	16	RSA/ECC/TDES/AES	I²C, USB 2.0, SPI, ISO7816	2.7 – 5.5	-40 / +105	SOIC8, QFN20
VaultIC420	32/112	RSA/ECC/TDES/AES	I²C, USB 2.0, SPI, ISO7816, RTC	1.62 – 5.5	-40 / +105	SOIC8, QFN44
VaultIC460	112	RSA/ECC/TDES/AES	I²C, USB 2.0, SPI, ISO7816, RTC	2.7 – 5.5	-40 / +105	SOIC8, QFN44

WISeKey
wisekey.com
info@wisekey.com