VaultIC186

Summary Datasheet

SEAL SQ
semiconductors + quantum

General Features

Cryptographic Services

- Public Key Pair Generation (ECC)
- Digital Signature
- Message Digest
- Deterministic Random Number Genertion

Cryptographic Algorithms

- ECC (GF2n) up to 283 bits

Software Features

- Mutual Strong Authentication
- Rights Management (Manufacturer, User)
- Secure File System
- Secure 32-bit Counters (Anti-Tearing with Anti-Stress)
- Host Public Key management (parsing, verification)

Memory

- File System 1.5 Kbytes (certificate, files and keyring)
- Write Endurance 500 Kcycles
- Data Retention 20 Years
- 2ms Program + 2ms Erase

Communication

- OWI (One Wire Interface)

Certifications / Standards

- Targeted Hardware Common Criteria EAL4+

Package

- 6-DFN (RoHS compliant) 2mm x 3mm

Hardware Platform

- Operating ranges : 1.62V to 5.5V
- 8-/16-bit RISC CPU
- Hardware Random Number Generator
- Hardware 16-bit Public Key Crypto Accelerator
- Low Power consumption: 64µA in standby mode and only 3 to 5mA during CPU-intensive operations
- Operating temperature : -40°C to +105°C

Timings

- Unilateral authentication of one device in less than 150ms (typical) : including Startup time and Internal Authenticate command with ECDSA B-163
- B233 Key-Pair Generation on-Chip in 770ms (typical)

Detailed Features

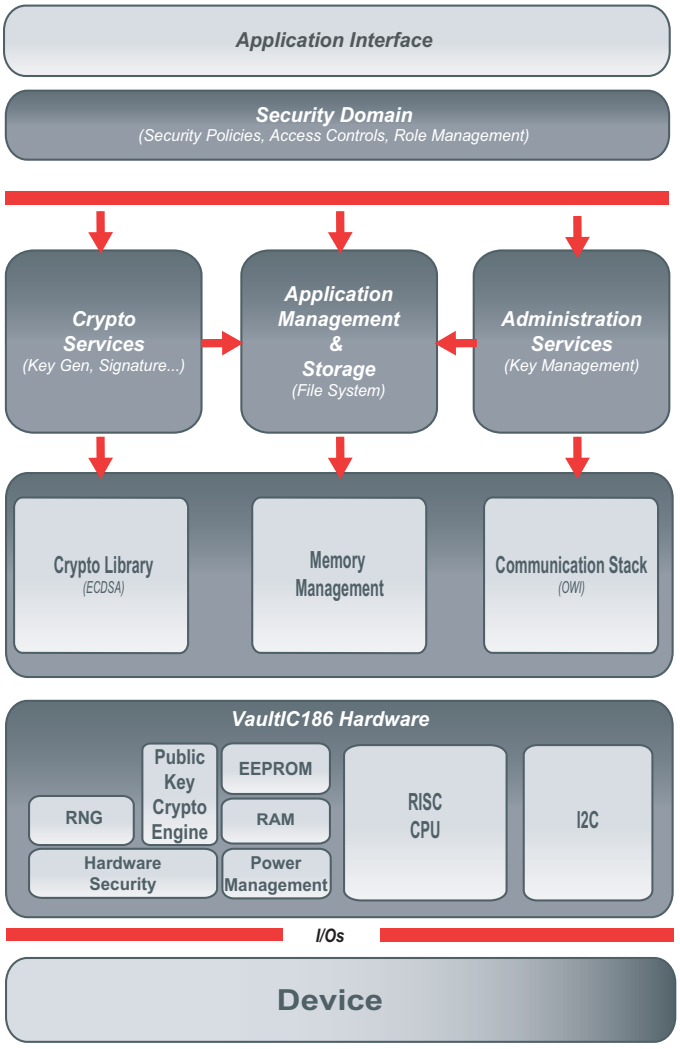
Description

The VaultIC186 is a Secure microcontroller solution designed to secure various systems against counterfeiting, cloning or identity theft. It is a hardware security module that can be used in many applications such as IP protection, access control or hardware protection.

The proven technology used in VaultIC186 security modules is already widespread and used in national ID/health cards, e-passports, bank cards (storing user Personal Identification Number, account numbers and authentication keys among others), pay-TV access control and cell phone SIM cards (allowing the storage of subscribers' unique ID, PIN code, and authentication to the network), where cloning must definitely be prevented.

Designed to keep contents secure and avoid leaking information during code execution, the VaultIC186 include voltage, frequency and temperature detectors, illegal code execution prevention, tampering monitors and protection against side channel attacks and probing. The chips can detect tampering attempts and destroy sensitive data on such events, thus avoiding data confidentiality being compromised. Strong Authentication capability, secure storage and flexibility thanks to its I²C interface, low pin count and low power consumption are main features of the VaultIC186. Its embedded firmware provides advanced functions such as Identity-based authentication, Cryptographic command set, ECC Public Key cryptographic algorithm, robust commmunication Protocol.

Figure 1 Software and Hardware Architecture



6654CS – 16Jan23

VaultIC186 includes 4 Secure 32-bit counters, for instance useful to avoid refilling of printers cartridge. These counters can be used in two ways: usual Counter mode or Direct mode, where each counter can be seen as small 32-bit files. These counters can also be used for authentication purpose.

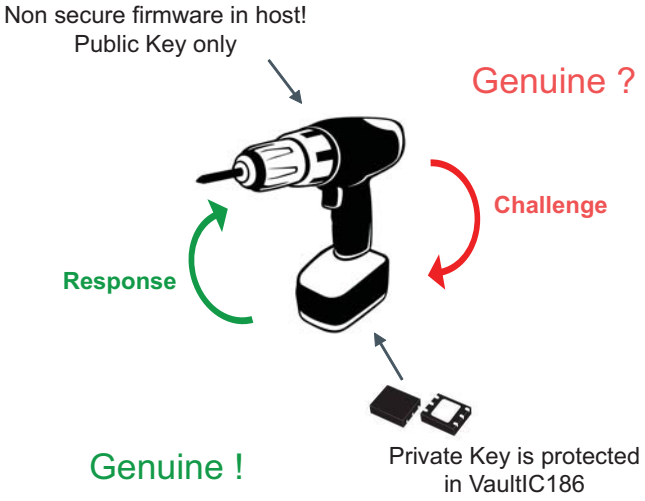
Thanks to the new dedicated feature parsing and verifying any Host certificate on-the-fly, the VaultIC183 can be used along with others VaultIC183 in the SEAL SQ's patented authentication mechanism ("Distributed cartridges authentication with diversified keypair"). Using this authentication mechanism up to ten products (such as cartridges) can be authenticated in less than 1 second with unique diversified keypair.

Asymmetric cryptography

To make the authentication possible, the VaultIC186 uses asymmetric cryptography. Contrary to the symmetric cryptography using the same key for encryption and decryption, the asymmetric cryptography uses a key pair (a Public key and a Private key), each for a specific purpose: the private key is for encryption, the public key for decryption.

Storing securely the Private Key, the VaultIC186 is capable to generate a unique digital signature that any host can verify using the associated Public Key. The main advantage of the asymmetric cryptography is the easy way of distributing keys : only the Private key should be protected and then the Host, embedding the Public key, does not need to be in a secure environment.

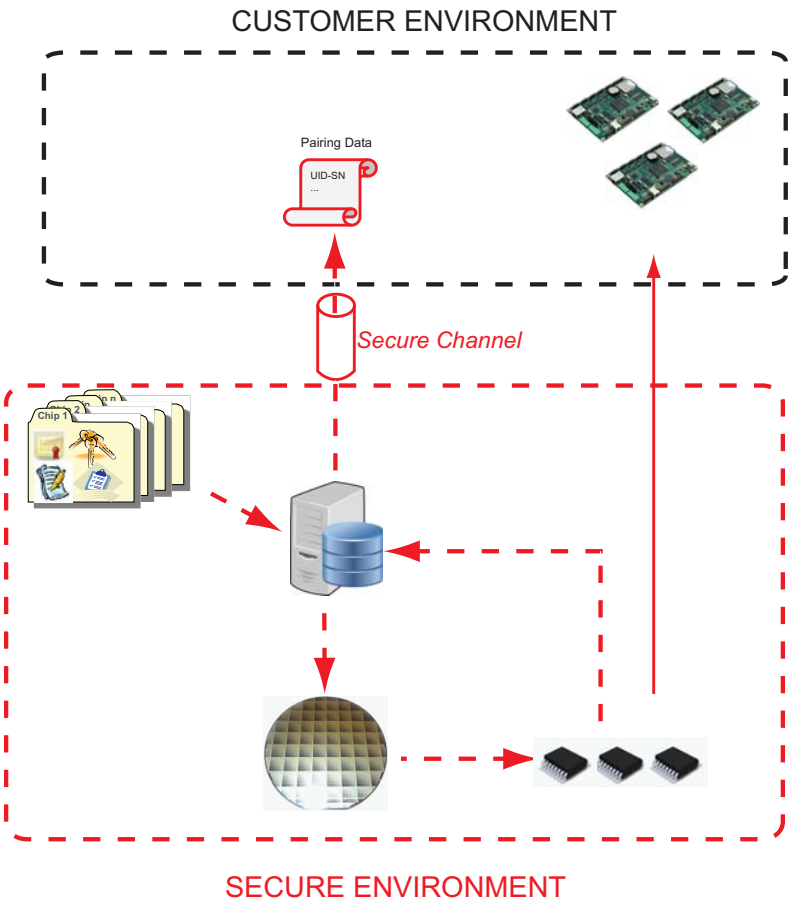
Figure 2 Asymmetric cryptography used in VaultIC186



Personalization

Thanks to VaultiTrust Generation and Provisionning service proposed by SEAL SQ, VaultIC186 devices can be personalized individually and in a secure environment: Keys and any other data are generated by SEAL SQ and inserted on each die at wafer level. Once assembled, all devices are provided to the customer as well as pairing data (Data inserted paired with Chip Serial Numbers).

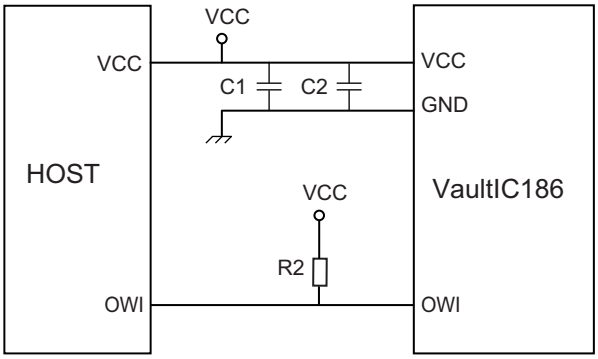
Figure 3 VaultiTrust Personalization service



For more information regarding VaultiTrust Personalization service, please contact your local SEAL SQ sales representative.

Product Characteristics

- Connections for Typical Application



- External components, Bill of Materials

Configuration	Reference	Description	Typical Values	Comment
OWI	C1	Power Supply Decoupling Capacitor	4.7 µF	Recommended
	C2	Power Supply Decoupling Capacitor	10 nF	Recommended
	R1	Pull-Up Resistors	2.2 kΩ	Recommended

- **Absolute Maximum Ratings**

Operating Temperature	-40°C to +105°C
Supply Voltage V_{cc}	-0.3V to +7.0V
Input Voltage	-0.3V to V_{cc}

Note: Stresses beyond those listed under “Absolute Maximum Ratings” may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or other conditions beyond those indicated in the operational sections of this specification is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

Ordering Information

- Legal
  - A **Non-Disclosure Agreement** must be signed with SEAL SQ.
  - An **Export License** for cryptographic hardware/software must be granted.

- Quotation and Volume
  - For minimum order quantity and the estimated annual utilization, please contact your local SEAL SQ sales representative.

- Part Number

Reference		Description
ATVAULTIC186-xxx-P		**xxx** : Chip “Chrono” Number* **P** = ZA : DFN6 Package
Reference	**Application**	**Description**
ATVAULTIC-STK04-186ZA	Embedded Security	Starter Kit for VaultIC186 in DFN6 package (WiseBoard included)

* For more details about the Chip “Chrono” Number, please contact your local SEAL SQ sales representative.

For Customer Data Insertion ordering, please add “**PERSO**” on the reference to be ordered.

Starter Kit

The VaultIC Starter Kit provides an easy path to master the cryptographic and secure data storage features of the VaultIC security modules. The content is :

- VaultIC186 samples (5 units) with 1 dedicated test socket
- 1 generic USB to OWI adapter board (WiseBoard)
- 1 USB key containing a support documentation set (getting started, application notes, reference design), some demo applications to get an insight into the VaultIC features, the ”VaultIC Manager” tool to design the file system and to personalize samples, a hardware independent cryptographic API with source code.

6654CS – 16Jan23

Pinout & Packaging

Designation	Pin	Description
GND	1	Ground (reference Voltage)
IO0	3	GPIO0. Used for OWI.
VCC	6	Power Supply

Figure 4 Pinout VaultIC186 in DFN6 package

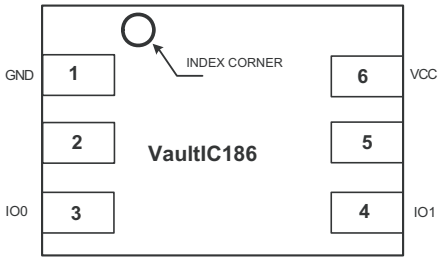
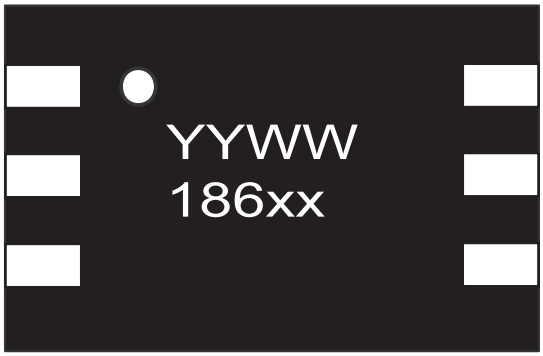
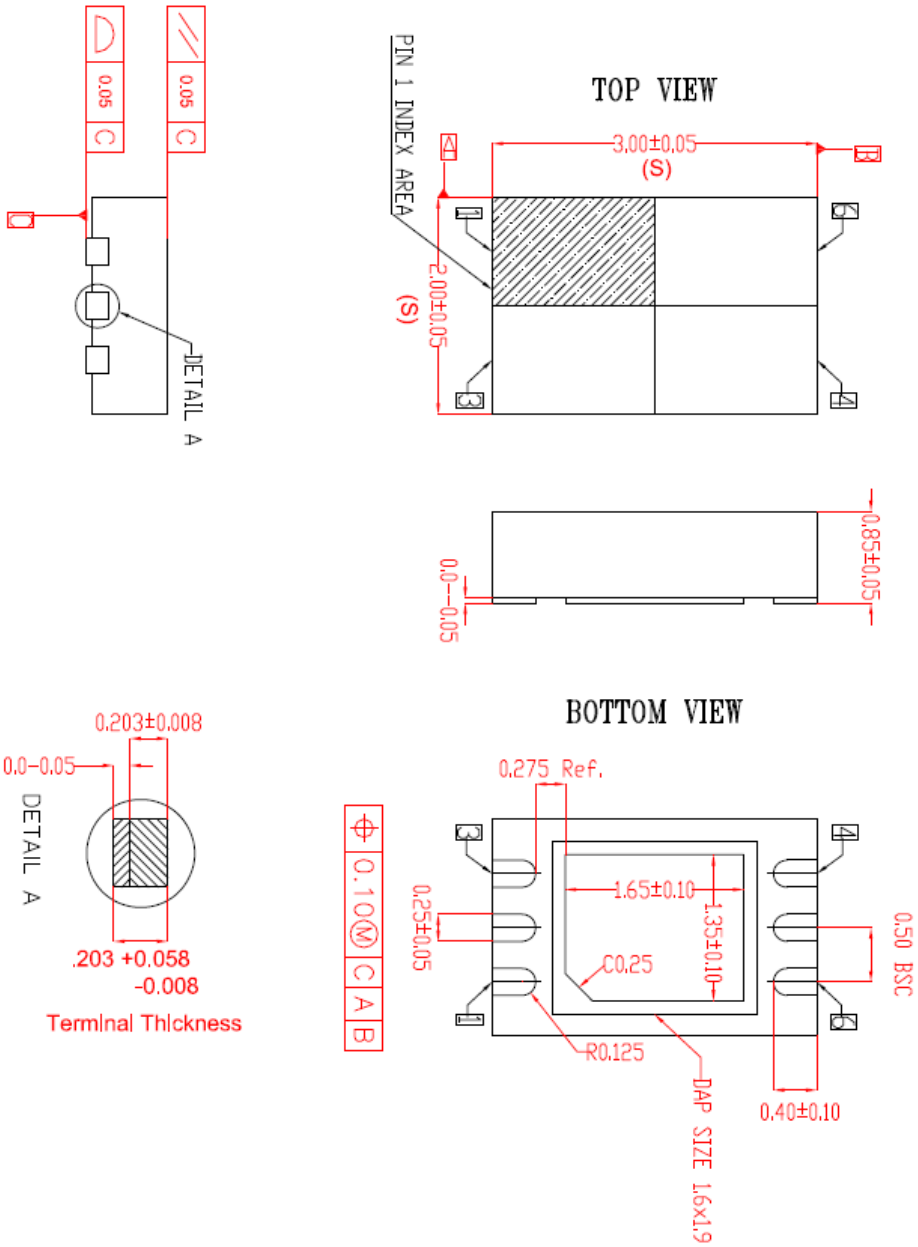


Figure 5 Product Marking



YYWW : Date Code
xx : Chip “Chrono” Number

Figure 6 Package DFN6



Notes:
1. All dimensions are in mm. Angles in degrees.
2. Coplanarity applies to the Exposed PAD as well as the terminals. Coplanarity shall not exceed 0.05mm.
3. Warpage shall not exceed 0.05mm.
4. Package length / Package width are considered as special characterisitic(s).
5. Refer JEDEC MO-229.

6654CS – 16Jan23