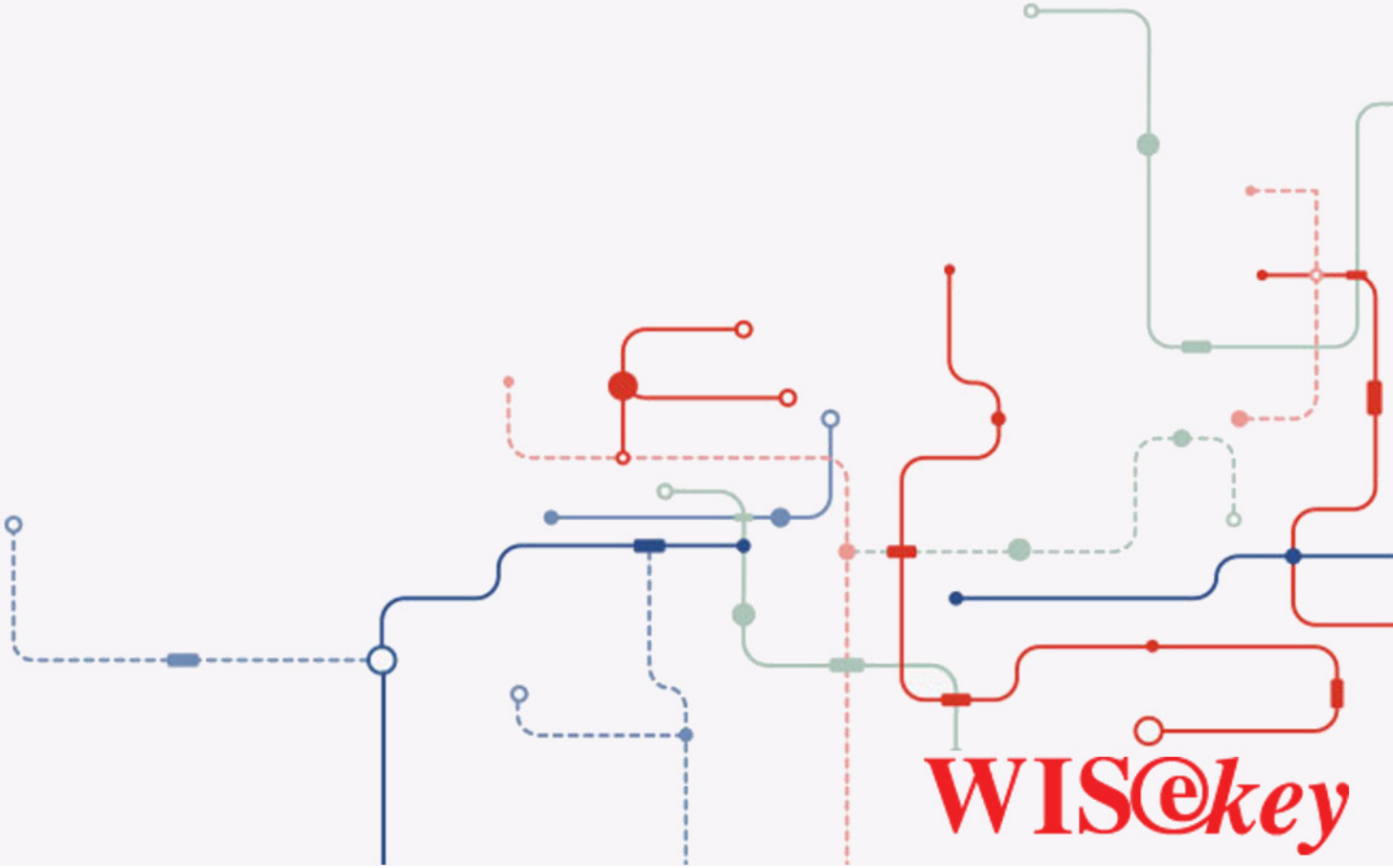
VAULTIC182

Summary Datasheet



General Features

Cryptographic Services

- Public Key Pair Generation (ECC)
- Digital Signature
- Message Digest
- Deterministic Random Number Generator (FIPS compliant)

Cryptographic Algorithms

- ECC ($GF2^n$) up to 303 bits, including FIPS recommended curves B233, K233, B283, K283

Software Features

- FIPS 140-2 Identity-based Authentication using Mutual Strong Authentication
- Rights Management (Manufacturer, User)
- Secure File System
- Secure 32-bit Counters (Anti-Tearing with Anti-Stress)

Memory

- File System 1.5 Kbytes (certificate, files and keyring)
- Write Endurance 500 Kcycles
- Data Retention 10 Years
- 2ms Program + 2ms Erase

Communication

- I²C (Two Wire Interface)
  - Bus speeds up to 100 kHz

Certifications / Standards

- Targeted Hardware Common Criteria EAL4+
- Targeted FIPS 140-2 Security Level 3

Packages

- 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 in less than 300ms (typical) in non-FIPS mode : including Startup time and Internal Authenticate command with ECDSA B-163
- B283 Key-Pair Generation on-Chip in 1.2 s (typical) in non-FIPS mode

6639CS – 22Feb19

Detailed Features

Description

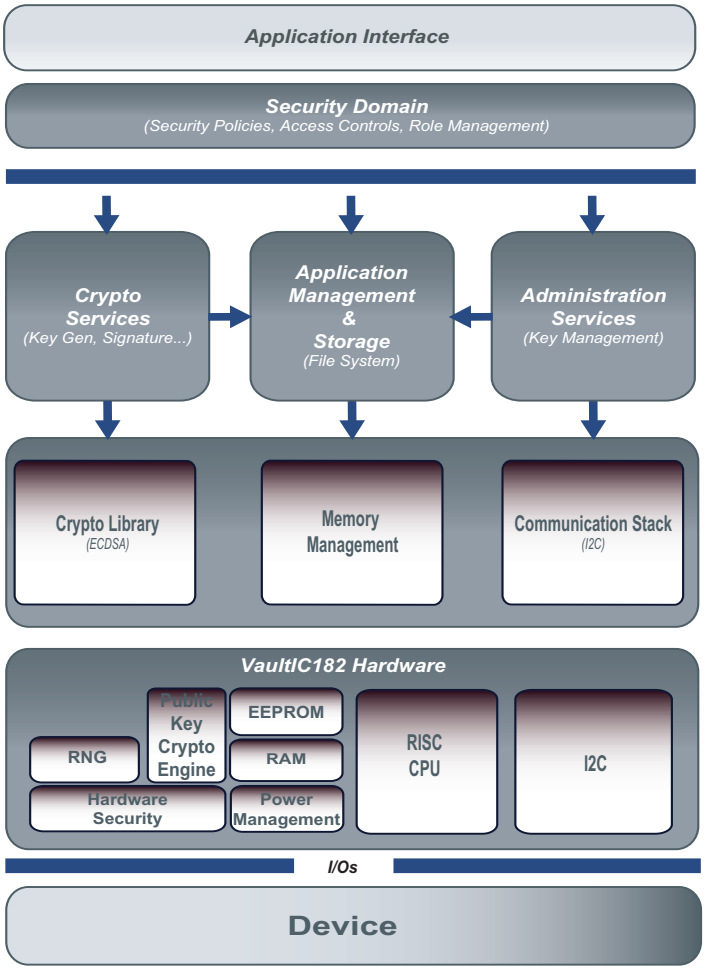
The VaultIC182 is a Secure microcontroller solution designed to secure various types of systems against counterfeiting, cloning or identity theft. It is a hardware security module that can be used in many applications such as IP protection, access control or hardware protection.

The proven technology used in VaultIC182 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 VaultIC182 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 the main features of the VaultIC182. Its embedded firmware provides advanced functions such as Identity-based authentication, Cryptographic command set, ECC Public Key cryptographic algorithm and robust communication Protocol.

VaultIC182 includes 16 Secure 32-bit counters, useful to avoid illegal refilling of printer cartridges for instance. Those 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 purposes.

Figure 1 Software and Hardware Architecture



Asymmetric cryptography

To make the authentication possible, the VaultIC182 uses Elliptic Curve Digital Signature Algorithm (ECDSA). Unlike the symmetric cryptography which uses the same key for cryptographic services, the asymmetric cryptography of ECDSA uses a key pair (a Public key and a Private key) for a specific purpose: the Private key for digital signature generation, the Public key for digital signature verification.

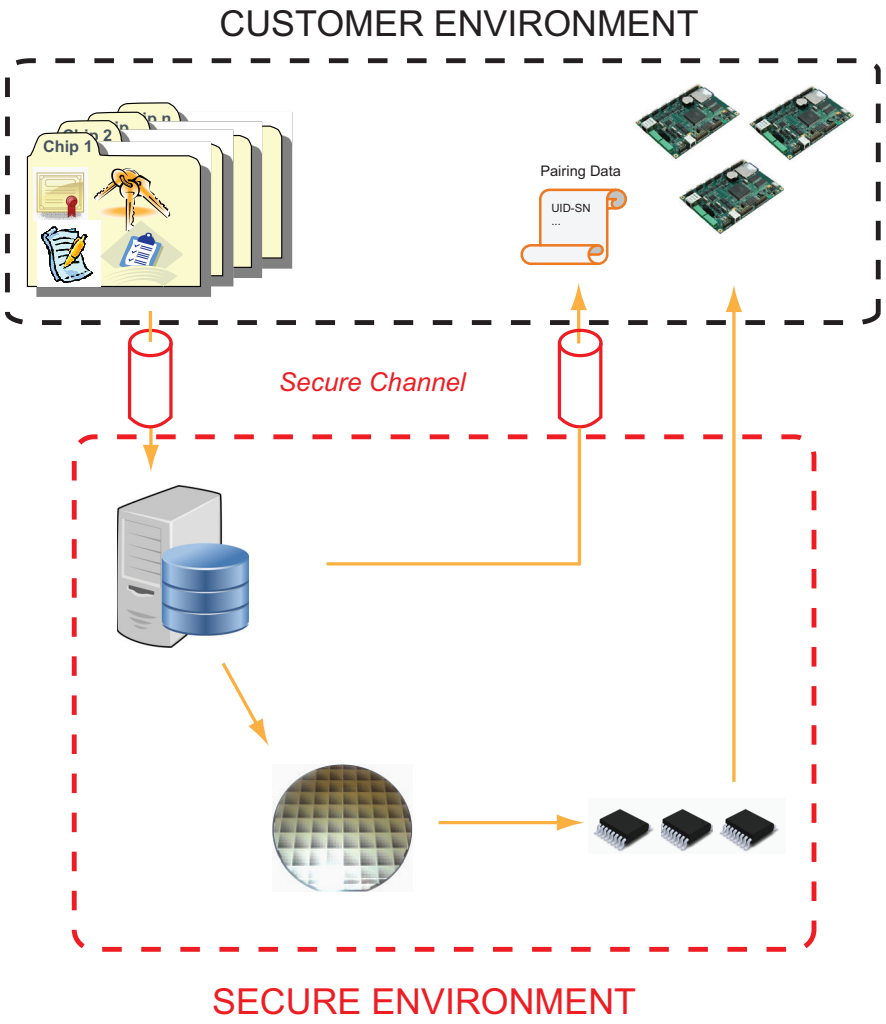
With a Private Key securely stored, the VaultIC182 is able to generate a digital signature that any host can verify using the associated Public Key. The main advantage of the asymmetric cryptography is the ease of distributing keys : only the Private key has to be protected and the Host, embedding the Public key, does not need to be in a secure environment.

Figure 2 Asymmetric cryptography used in VaultIC182

Personalization

Thanks to VaultiTrust Personalization service proposed by WISeKey, VaultIC182 devices can be personalized individually and in a secure environment: Customer Keys and any other data are submitted to WISeKey through a secure channel then inserted on each die at wafer level. Once assembled, all devices are provided to the customer as well as pairing data (Customer Data inserted paired with Chip Serial Numbers).

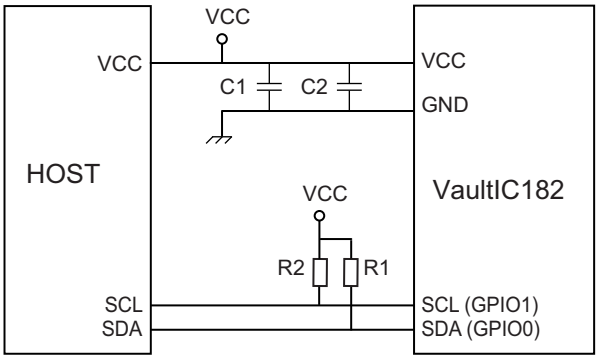
Figure 3 VaultiTrust Personalization service



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

Product Characteristics

• Connections for I²C Typical Application



• External components, Bill of Materials

Configuration	Reference	Description	Typical Values	Comment
I²C	C1	Power Supply Decoupling Capacitor	4.7 µF	Recommended
	C2	Power Supply Decoupling Capacitor	10 nF	Recommended
	R1, R2	Pull-Up Resistors	2.2 kΩ	Recommended

• I²C Timings

The table below describes the requirements for devices connected to the I²C Bus.

Symbol	Parameter	Condition	Min.	Typ.	Max.	Unit
f_{SCL}	SCL Clock Frequency	-	-	-	100	kHz

• 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 WISeKey.
  - 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 WISeKey sales representative.
- **Part Number**

Reference		Description
ATVAULTIC182-xxx-P		**xxx** : Chip “Chrono” Number* **P** = ZA : DFN6 Package
Reference	**Application**	**Description**
ATVAULTIC-STK02-182ZA	Embedded Security	Starter Kit for VaultIC182 in DFN6 package (I²C adapter included)
ATVAULTIC-STK12-182ZA	Embedded Security	Starter Kit for VaultIC182 in DFN6 package (no I²C adapter)

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

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 :

- VaultIC182 samples (5 units) with 1 dedicated test socket
- 1 generic USB to I²C adapter
- 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.

Figure 4 Starter Kit Content

6639CS – 22Feb19

Pinout & Packaging

Designation	Pin	Description
GND	1	Ground (reference Voltage)
IO0	3	GPIO0. Used for SDA
IO1	4	GPIO1. Used for SCL
VCC	6	Power Supply

Figure 5 Pinout VaultIC182 in DFN6 package

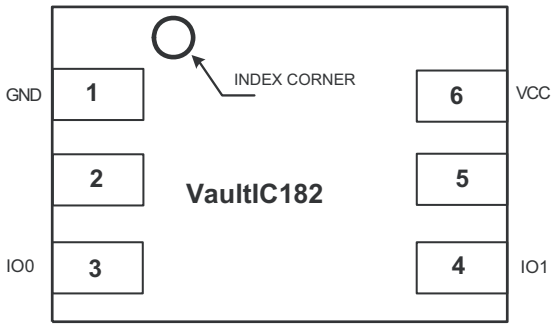
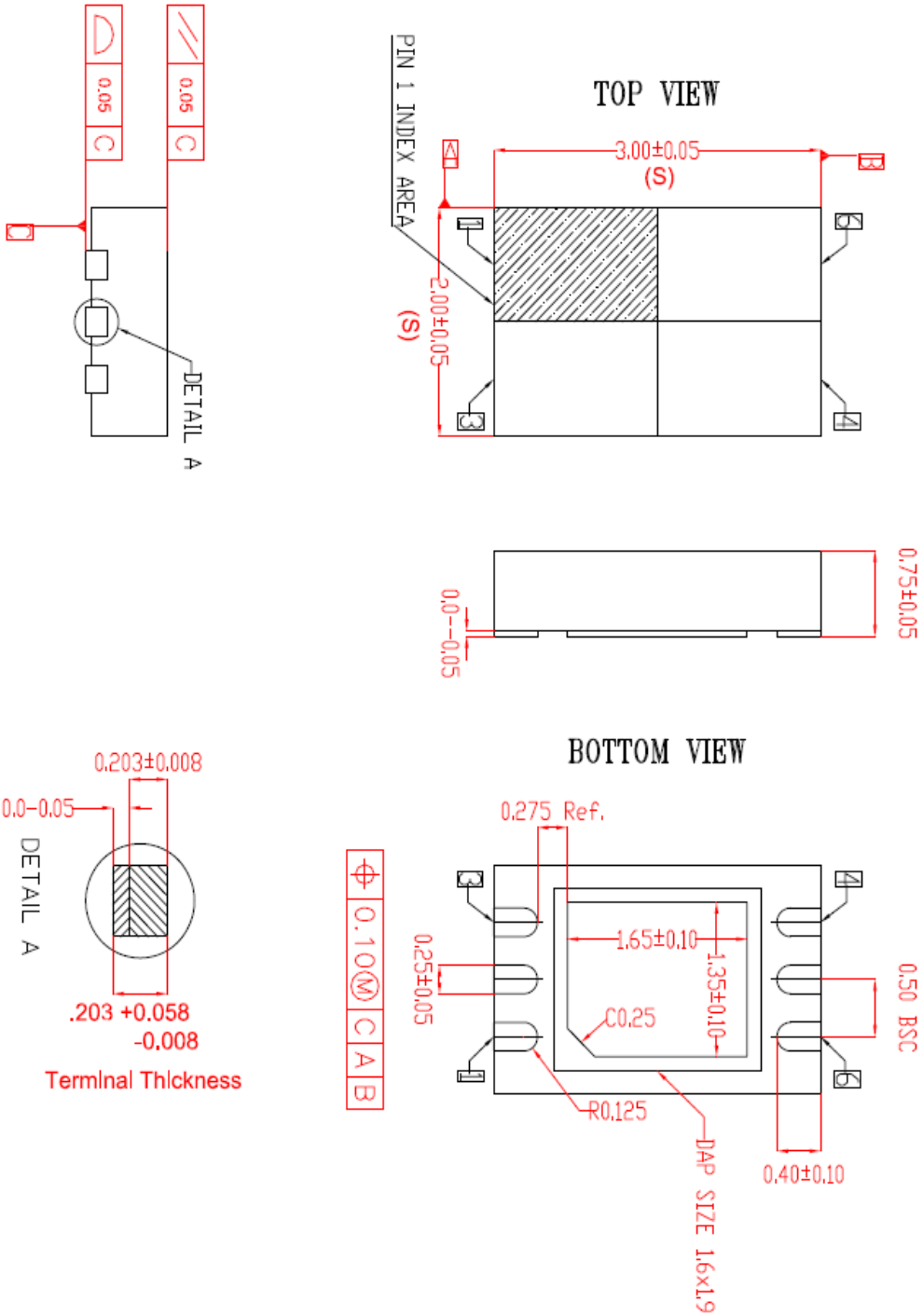


Figure 6 Product Marking

YYWW : Date Code
xx : Chip “Chrono” Number

Figure 7 Package Thin 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.

6639CS – 22Feb19