VAULTIC292

Summary Datasheet

SEAL SQ
semiconductors + quantum

General Features

Cryptographic Services

- Private-public key pair generation
- Digital signature (ECDSA) generation
- Digital signature (ECDSA) verification
- ECDH shared secret generation
- True Random Number Generation

Cryptographic Algorithms

- ECC NIST P-256 curve (secp256r1)

Software Features

- Lifecycle CREATION and ACTIVATED modes
- Host and SE secret exchanges protected with a rotating key mechanism (pairing mode)
- Tearing protection on critical data
- Tamper attack detection

Memory

- 1680-byte secure storage area
  - can store ECC P-256 keys and certificates
  - e.g. 5 key pairs + 2 full X509 certificates
  - data retention 20 years
- RAM secured key ring area - stores up to 3 ECC P-256 ephemeral key pairs

Communication

- I²C (Two Wire Interface)
  - Bus speed up to 400kHz

Certifications / Standards

- Hardware: EAL5+ ready
- True RNG: NIST SP 800-90A, NIST SP 800-90B
- ECDSA: FIPS 186-4
- ECC Parameters: NIST SP 800-186

Package

- UDFN8 (RoHS compliant) 2mm x 3mm x 0.5mm
- DFN6 (RoHS compliant) 2mm x 3mm x 0.75mm

Hardware Platform

- Operating range : 1.62V to 5.5V
- 8-/16-bit RISC CPU
- Hardware Random Number Generator
- Hardware 16-bit Public Key Crypto Accelerator
- Power consumption: 100µA in standby mode and 3 to 5mA during CPU-intensive operations
- Operating temperature : -40°C to +105°C

Timings

- Start up time less than 100ms

Typical applications

- Secure provisioning of birth certificate / digital identities
- Secure connection to Clouds & Device To Device Authentication through TLS 1.2 & 1.3 (WolfSSL, MbedTLS)
- Firmware signature verification for Secure Boot

- Anti-Counterfeiting
- Smart Home (Matter) / Smart Cities / Smart Industry
- USB-C Device Authentication
- QI Power Transmitter Authentication

6656CS – 16May23

Detailed Features

Description

The VaultIC292 is a secure microcontroller designed to bring a robust & unique digital identity to a device, essential for applications, such as:

- Creating a secure connection to a cloud or a local network using e.g. TLS
- Authenticating a USB-C device
- Authenticating a QI power transmitter

It provides the essential cryptographic functions and protects related private keys against tampering.

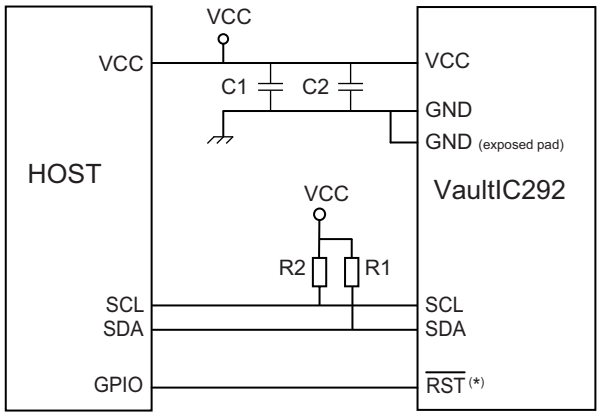
Moreover, when pre-personalized during SEALSQ's secure production process VaultITrust, with a digital identity tailored to be used for connection to AWS, Azure or a private cloud, the VaultIC292 will ease device manufacturing and logistics chain in a zero-trust environment.

VaultIC292 is built on technology that has proven its strength in National ID cards, e-Passports, Bank cards, Pay-TV Access Control cards and IoT applications.

6656CS – 16May23

Product Characteristics

- Connections for Typical Application



* DFN6 only

- External components, Bill of Materials

Reference	Description	Typical Values	Comment
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	400	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 SEALSQ.
  - An **Export License** for cryptographic hardware/software must be granted.

- Quotation and Volume
  - For minimum order quantity and the estimated annual usage, please contact your local SEALSQ sales representative.

- Reference number

Reference	Description
VAULTIC292-xxx-ZA	**xxx** : Chip “Chrono” Number(*)
VIC292_TLS_RPI_STK	Starter Kit for VaultIC292

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

Starter Kit

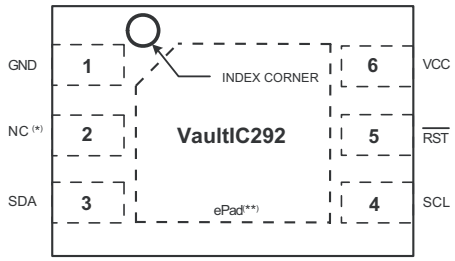
The VaultIC292 Starter Kit provides an easy path to master the cryptographic and secure data storage features of the VaultIC292 security modules. The content is :

- 1 board with soldered VaultIC292 dedicated to be plugged on an RaspBerry board
- 1 USB key containing support documentation (getting started, application notes, reference design), C-Source code API and demo applications aloowing an easy integration of VaultIC292 in host systems.

6656CS – 16May23

DFN6 Pinout & Packaging

Figure 1 Pinout - top view



* not connected: the pin can be freely left floating, or connected to GND, or connected to VCC

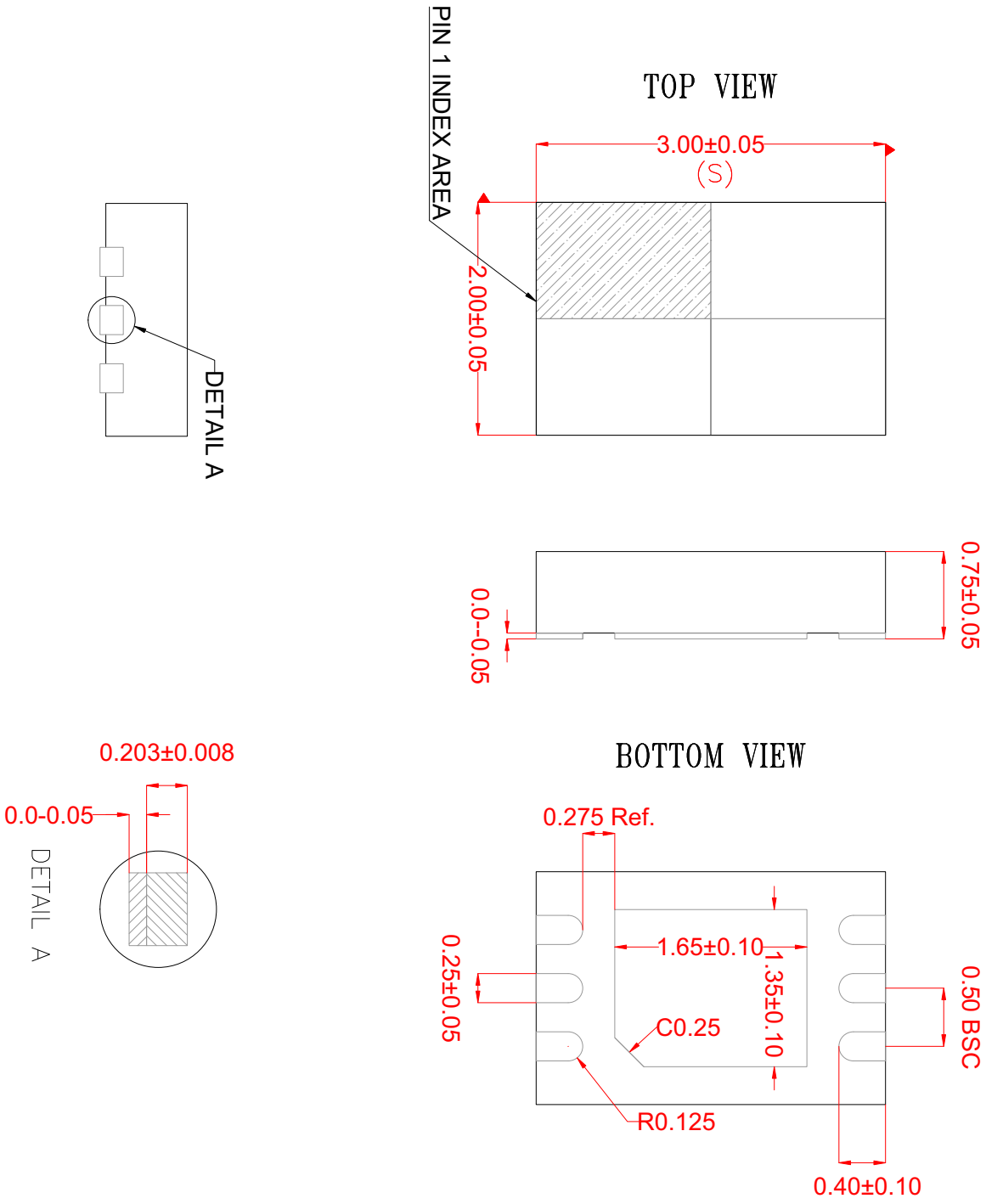
** exposed pad: not internally connected (floating). It is recommended, but not mandatory, to connect it to the board GND

Designation	Pin	Description
GND	1	Ground (reference Voltage)
SDA	3	I^2C data
SCL	4	I^2C clock
$\overline{RST}$	5	Reset
VCC	6	Power Supply

Figure 2 Product marking - top view

YYWW : Date Code

Figure 3 DFN6 package outline



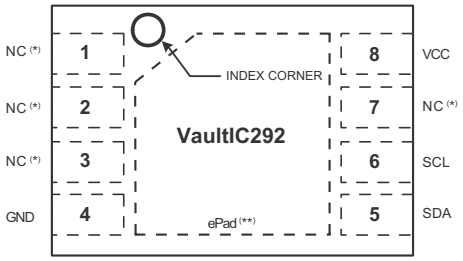
Notes

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.

6656CS – 16May23

UDFN8 Pinout & Packaging

Figure 4 Pinout - top view



* not connected => the pin can be freely left floating, or connected to GND, or connected to VCC

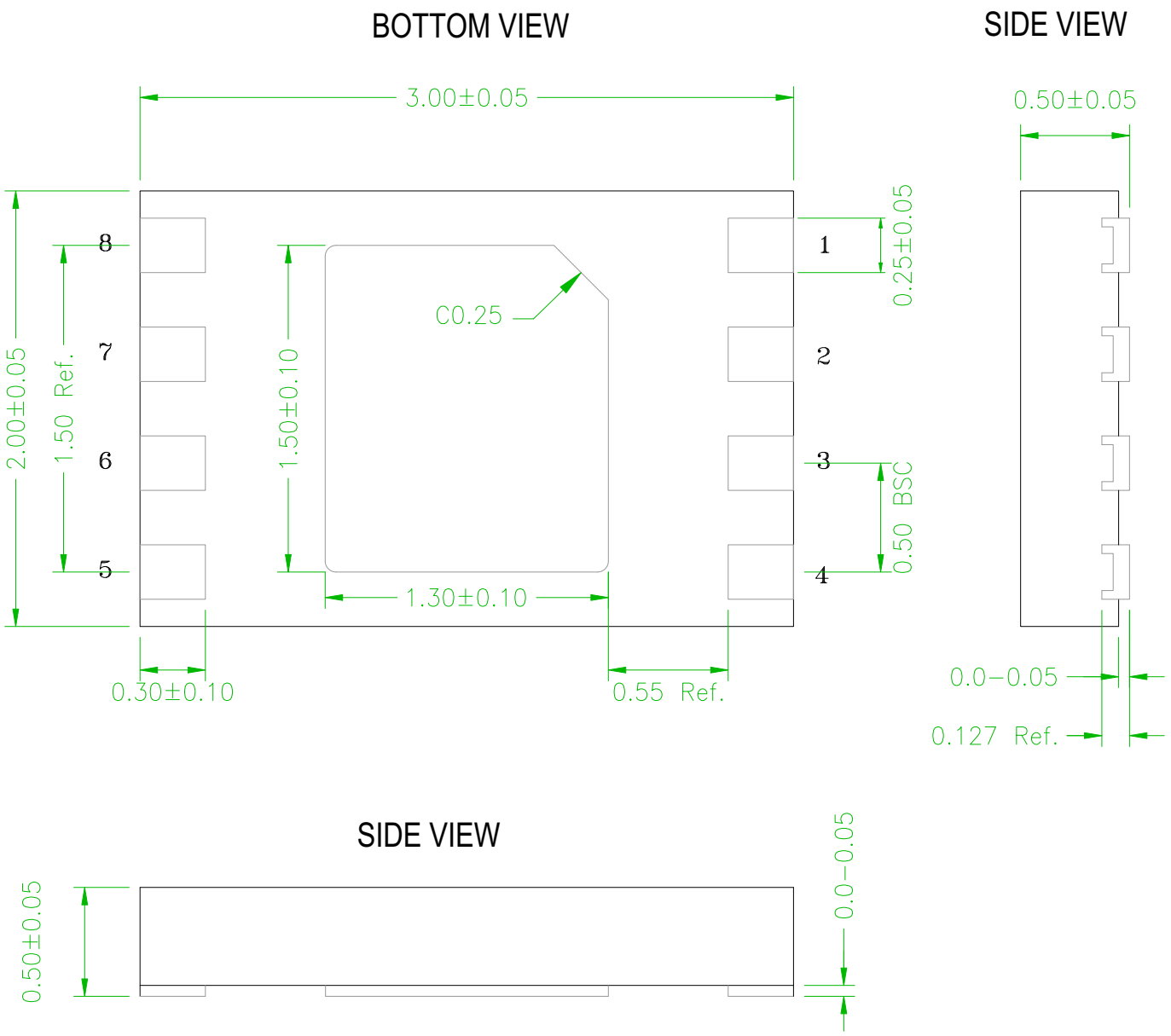
** the exposed pad is internally connected to GND. It is recommended (but not mandatory) to connect it to the board GND

Designation	Pin	Description
GND	4	Ground (reference Voltage)
SDA	5	I^2C data
SCL	6	I^2C clock
VCC	8	Power Supply

Figure 5 Product marking - top view

YYWW : Date Code

Figure 6 UDFN8 package outline



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 0.08mm.
3. Warpage shall not exceed 0.10mm.
4. Package length / Package width are considered as special characterisitic(s).
5. Refer JEDEC MO-220.