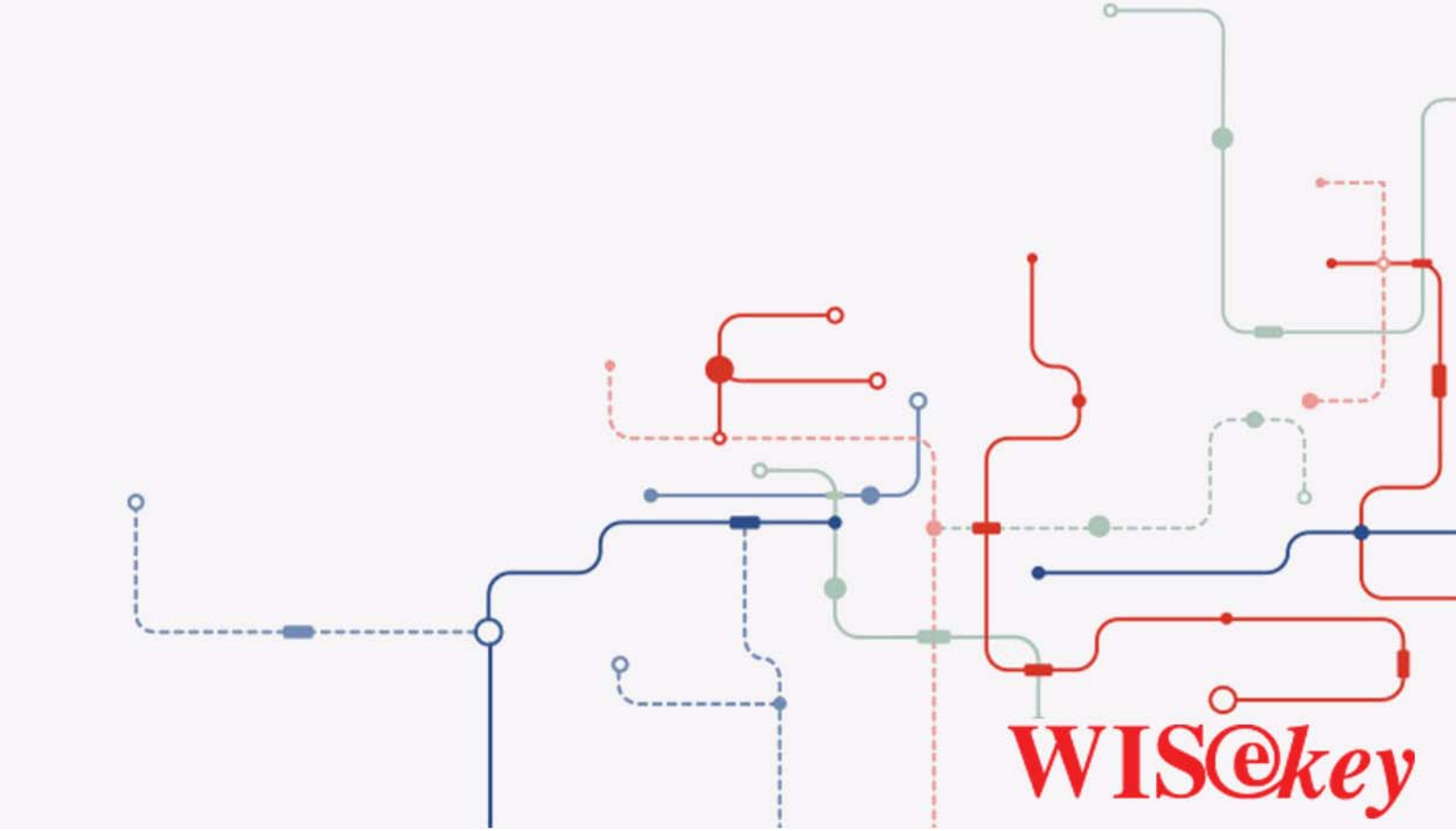
VAULTIC407

Summary Datasheet



General Features

Cryptographic Services

- Public Key Pair Generation
- Digital Signature Generation / Verification
- Encryption / Decryption
- Message Digest
- Key Wrapping / Unwrapping
- True Random Number Generation

Cryptographic Algorithms

- AES 128/192/256 bits
- GCM / GMAC
- RSA® up to 4096 bits*
- DSA up to 2048 bits
- ECC up to 576 bits over GF(p) and GF(2^m)

*Key sizes supported:
- Linear key size up to 2888 bits for CRT format only (2240 bits otherwise)
- 4096 bits for: CRT only Private exponent, Public exponent, CRT key generation.

Software Features

- FIPS 140-2 Identity-based authentication using password, Strong Authentication with Secure Channel Protocol (SCP03) and Certificate Based Authentication (SCP11)
- Rights Management (Administrator, Approved User, Non-approved User...)
- Embedded Dynamic File System

Memory

- Up to 16Kb dedicated to the File System
- EEPROM Write Endurance : 500 Kcycles
- EEPROM Data Retention : 20 Years
- 7-Slot ephemeral Key Ring

Communication

- Slave SPI Serial Interface, WISeKey's Proprietary Protocol
- I²C (Two Wires Interface), WISeKey's Proprietary Protocol

Package

- SOIC8 (RoHS compliant) 5mm x 5mm

Hardware Platform

- 8-/16-bit RISC CPU
- Hardware Random Number Generator
- Hardware AES 128/192/256 Engine DPA/DEMA Resistant
- Hardware 32-bit Public Key Crypto Co-Processor
- CRC 16 & 32 Engine (Compliant with ISO / IEC 3309)

Security

- Dedicated Hardware for Protection Against SPA/DPA/SEMA/DEMA Attacks
- Advanced Protection Against Physical Attack, including Active Shield, Enhanced Protection Object, CStack Checker, Slope Detector, Parity Errors (ROM, RAM)
- Environmental Protection Systems
- Voltage Monitor
- Frequency Monitor
- Temperature Monitor
- Light Protection
- Code Signature Module

Certifications / Standards

- EAL5+ Ready
- NIST CAVP
- SSL support
- TLS support
- PKCS#11

6646BS – 25Sept19

1. Overview

The VaultIC407 is a secure microcontroller-based 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 VaultIC407 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.

Strong Authentication capability, secure storage and flexibility thanks to the various interfaces (SPI, I²C), low pin count and low power consumption are main features of the VaultIC407. Its embedded firmware provides advanced functions such as Role-based access control, large Cryptographic command set, various Public domain cryptographic algorithms, Cryptographic protocols, Secure Channel Protocols, Robust communication protocol.

1.1 Tamper resistance

WISeKey's security modules will advantageously replace complex and expensive proprietary anti-tampering protection system. Their advantages include low cost, ease of integration, higher security and proven technology.

They are designed to keep contents secure and avoid leaking information during code execution. While on regular microcontrollers, measuring current consumption, electromagnetic emissions and other side channels may give precious information on the processed data or allow the manipulation of the data. WISeKey's secure microcontrollers' security features 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 erase sensitive data on such events, thus avoiding data confidentiality being compromised.

These features make cryptographic computations secure in comparison with regular microcontrollers whose memories can be easily duplicated. It is much safer to delegate cryptographic operations and storage of secret data (keys, identifiers, etc.) to a WISeKey microcontroller.

6646BS – 25Sept19

1.2 Authentication capability

The methods to authenticate humans are generally classified into three cases: physical attribute (e.g. fingerprint, retinal pattern, facial scan, etc.), security device (e.g. ID card, security token, software token or cell phone) and something the user knows (e.g. a password/passphrase or a personal identification number).

To fight against identity theft, the multi-factor authentication is a stronger alternative to the classical login/password authentication (called weak authentication). It combines two or more authentication methods (often a password combined with a security token). Two-factor systems greatly reduce the likelihood of fraud by requiring the presence of a physical device used together with a password. If the physical device is lost or the password is compromised, security is still intact. NIST's authentication guideline can be referred to for further details.

Multi-factor authentication requires a strong authentication. Anticloning is safely implemented through one-way or mutual strong authentication. Various authentication protocols exist (as specified in ISO9798-2 or FIPS196), but the main method is the **challenge-response authentication**:

1. The authenticator sends a challenge (e.g. a random number) to the equipment that must be authenticated ("the claimant").
2. The claimant computes a digital signature of the combination of this challenge with an optional identifier, using a private or secret key. The requested signature is then returned to the authenticator.
3. The authenticator checks the signature using either the same secret key or the public key associated to the claimant's private key and decides whether the claimant is authorized or not based on the signature verification result.

This strong authentication method requires storing secret data. Pure software multi-factor solutions are thus not reliable.

1.3 Secure storage

If sensitive data is stored in files on a hard disk, even if those files are encrypted, the files can be stolen, cloned and subjected to various kinds of attacks (e.g. brute force or dictionary attack on passwords). Therefore secure microcontroller-based hardware tokens are a must. Placing secrets outside the computer avoids risking exposure to malicious software, security breaches in web browsers, files stealing, etc.

1.4 Flexibility

The VaultIC407 product features:

- Various **communication interfaces** including SPI (Serial Protocol Interface) and I²C (Two Wires Interface) .
- **Low pin count** (Vcc, GND, and communication interface specific pins) making integration into an existing board simple. VaultIC407 modules are available in small package (SOIC8) to fit into the most size-constrained devices.
- **Low power consumption**, in order to extend battery life in portable devices and low-power systems. VaultIC407 devices consume less than 300µA in standby mode, and only 10 to 20mA (see Table 3-2) during CPU-intensive operations depending on the required action.

- **Embedded firmware** that provides advanced functions:
  - *Secure storage*: a fully user-defined non-volatile storage of **16KBytes** for sensitive or secret data.
  - *Role-based access control* with user, administrator and manufacturer roles supported.
  - *Cryptographic command set* to perform cryptographic operations using keys and data from the file system including: authentication, digital signature, encryption/decryption, hash, one-time password generation, random generation and public key pair generation.
  - *Public domain cryptographic algorithms* such as AES, RSA PKCS#1 v2.1, DSA, EC-DSA, MAC using AES
  - *Cryptographic protocols* such as secret-key unilateral or mutual authentication and public key based unilateral or mutual authentication .
  - *Secure Channel Protocol* using AES and key agreement.
  - *Robust communication protocol* stacked over the physical communication interfaces.
  - Starter Kit with RSA PKCS#11 libraries.

1.5 Ordering Information

1.5.1 Legal

A **Non-Disclosure Agreement** must be signed with WISeKey.

An **Export License** for cryptographic hardware/software must be granted.

1.5.2 Quotation and Volume

For minimum order quantity and the annual volume, please contact your local WISeKey sales office.

1.5.3 Part Number

Reference		Description
VAULTIC407-xxx-P		**xxx** : Chip “Chrono” Number* **P** =R : SOIC8 Package
Reference	**Application**	**Description**
VAULTIC-STK02-407R	Embedded Security	Starter Kit for VaultIC407 in SOIC8 package - SPI/I²C configuration
VAULTIC-STK12-407R	Embedded Security	Starter Kit for VaultIC407 in SOIC8 package - SPI/I²C configuration (SPI/I²C adapter not included)

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

1.5.4 Starter Kit

The VaultIC407 Starter Kit provides an easy path to master the cryptographic and secure data storage features of the VaultIC407 secure modules. The content is :

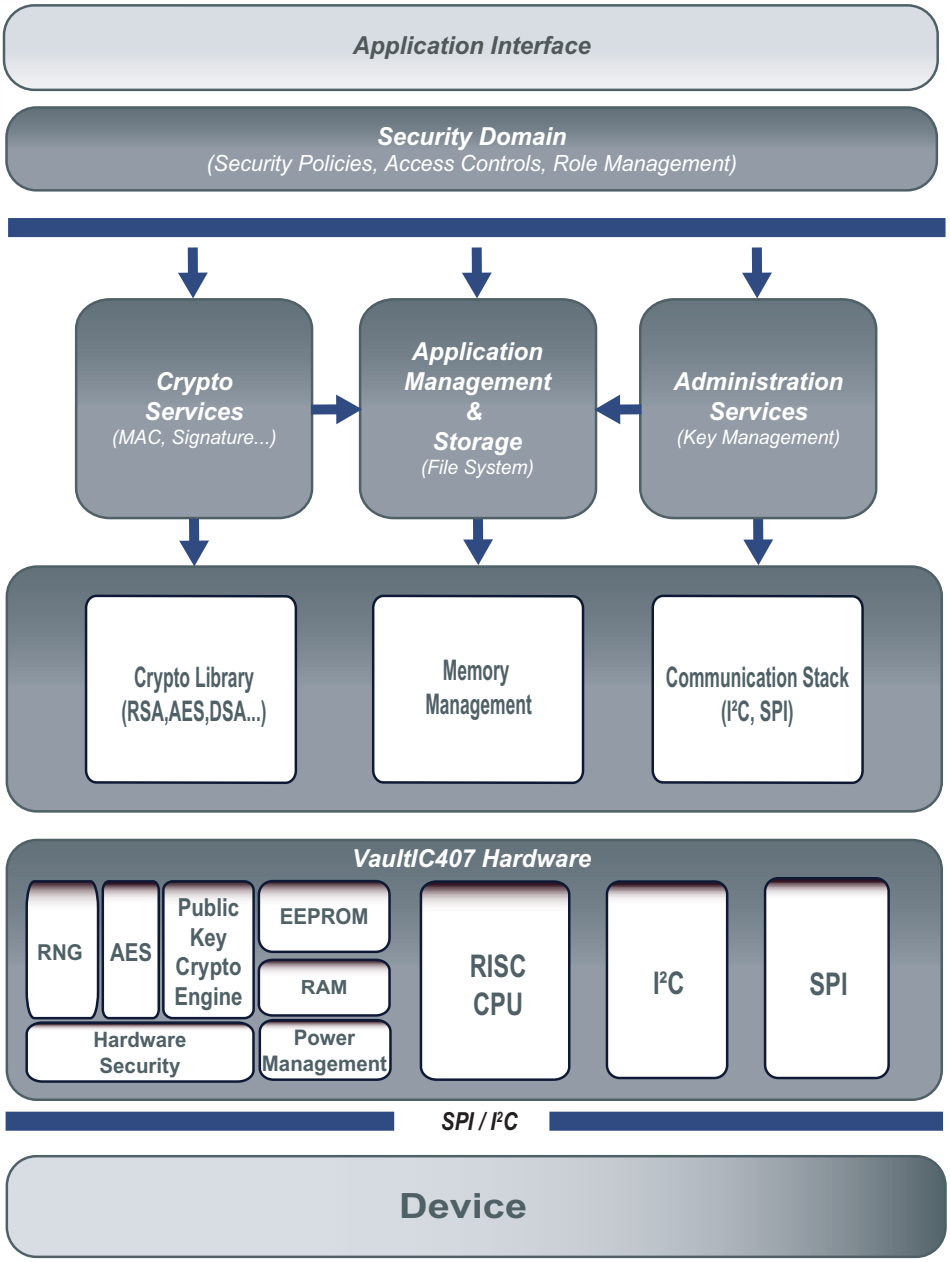
- VaultIC407 samples with 1 dedicated test socket
- 1 generic USB to SPI / I²C adapter (optional)
- 1 USB key containing a support documentation set (getting started, application notes, reference design), some demo applications to get an insight into the VaultIC4xx features, the ”VaultIC Manager” tool to design the file system and to personalize samples, a hardware independent cryptographic API with source code, libraries such as PKCS#11.

Figure 1-1. Starter Kit VaultIC407 - Example of content

1.6 Software and Hardware Architecture

The VaultIC407 software architecture is as shown on the diagram below.

Figure 1-2. Software and Hardware Architecture



2. Detailed Features

2.1 Communication Interfaces

The VaultIC407 embeds the following communication interfaces:

- **SPI**: up to 13 Mbps
- **I²C** : up to 400 kbps

2.2 Security Mechanisms

The table below summarizes the cryptographic algorithms supported by the VaultIC407.

Please refer to the document *VaultIC407 Technical Datasheet* (Available under Non-Disclosure Agreement only) for more details.

Table 2-1. Supported Algorithms table

Cryptographic Services	Supported Algorithms
Strong Authentication	• Password authentication Generic challenge-response authentication protocol using digital signatures • ISO/IEC 9798-2 • FIPS 196 • Global Platform v2.2 SCP03 using AES • Global Platform v2.2 SCP11 using AES and ECC
Public Key-Pair Generation	• PKCS#1.5 RSA keypair generator • FIPS 186-4 DSA keypair generator • FIPS 186-4 ECDSA keypair generator
MAC (Message Authentication Codes)	• NIST SP 800-38B AES CMAC • NIST SP 800-38D AES GMAC • FIPS 198-1 HMAC with SHA-1, SHA-224, SHA-256, SHA-384 or SHA-512
Message Signature	• PKCS#1 v2.1 RSASSA PSS • PKCS#1 v2.1 RSASSA-PKCS1-v1_5 • Raw RSA X.509 with no padding • FIPS 186-4 DSA • FIPS 186-4 ECDSA over GF(p) and GF(2^m) • ECDSA-GBCS

Cryptographic Services	Supported Algorithms
Message Encryption	Data encryption / decryption: • AES • PKCS#1 v2.1 RSAES-OAEP • PKCS#1 v2.1 RSAES-PKCS1-v1.5 • Raw RSA X509 with no padding
	Block chaining modes: • ECB • CBC • OFB • CFB (CFB-128 for AES) • CTR
	Padding methods: • No padding • Method 1 • Method 2 • PKCS 5 • PKCS 7
Authentication - Cipher	• AES-GCM 128-192-256 bits
HOTP - One-Time Password Generation	• OATH Hash-based OTP algorithm (RFC 4226) • OATH Time-based OTP algorithm (Draft v5)
Message Digest	• SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512
Random Number Generation	• NIST SP 800-90 Deterministic Random Bit Generator using CTR-AES-256 algorithm
Key Transport Scheme	• NIST SP800-56B Key Transport Scheme based on RSAES-OAEP without key confirmation • Generic Key Transport Scheme based on AES
Key Agreement Protocol	Key agreement schemes based on Elliptic Curves featuring in accordance with: • ANSI X9.63 • NIST SP800 56Ar2 • BSI-TR-03111

6646BS – 25Sept19

Cryptographic Services	Supported Algorithms
Key Establishment Primitives	• ECC_DH according to ANSI X9.63 • ECC_CDH according to ANSI X9.63 and NIST SP800 56Ar2 • ECKA according to BSI-TR-03111
Key Derivation Function	• KDF_CONCATENATION according to NIST SP800 56Ar2 • KDF_X963 according to ANSI X9.63 • KDF_HASH according to Microsoft Smart Card Minidriver specification
Key Confirmation	Supported by Key Agreement Protocol in FIPS mode

3. Product Characteristics

3.1 Maximum Ratings

Table 3-1. Absolute Maximum Ratings

Symbol	Parameter	Min.	Max.	Units
V_{CC}	Supply Voltage	-0.3	7.5	V
V_{IN}	Input Voltage	V_{SS}-0.3	V_{CC}+0.3	V
T_A	Operating Temperature	-40	+105	°C
E_{EEPROM}	EEPROM Endurance for write/erase cycles		500 000 (1)	cycles
$t_{DataRetention}$	EEPROM Data Retention		50 (2)	Years
ESD	Electrostatic Discharge		4(HBM) 1(CDM)	kV
Lup	Latch-up		+/- 200	mA

1. At a temperature of 25°C.
2. Failure rate <1 ppm at a temperature of 25°C

Caution

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.

3.2 AC/DC Characteristics (2.7V - 5.5V range; T= -40°C to +105°C)

Table 3-2. AC/DC Characteristics (2.7V - 5.5V range; T= -40°C to +105°C)

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
V_{CC}	**Supply Voltage**		2.7		5.5	V
V_{IH}	**Input High Voltage** - SPI_MISO, SPI_MOSI, SPI_SCK, SPI_SEL, SPI_SS, GPIOs		0.7*V_{CC}		V_{CC}+0.3	V
V_{IL}	**Input Low Voltage** - SPI_MISO, SPI_MOSI, SPI_SCK, SPI_SEL, SPI_SS, GPIOs		-0.3		0.2*V_{CC}	V
I_{IH}	**Leakage High Current** - SPI_MISO, SPI_MOSI, SPI_SCK, SPI_SEL, SPI_SS, GPIOs	V_{IN} = V_{IH}	-10		10	µA
I_{IL}	**Leakage Low Current** - SPI_MISO, SPI_MOSI, SPI_SCK, SPI_SEL, SPI_SS, GPIOs	V_{IN} = V_{IH}	-40		10	µA
V_{OL}	**Output Low Voltage** - SPI_MISO, SPI_MOSI,SPI_SCK, SPI_SS, GPIOs	I_{OL} = 1mA	0		0.1*V_{CC}	V
V_{OH}	**Output High Voltage** - SPI_MISO, SPI_MOSI,SPI_SCK, SPI_SS, GPIOs	I_{OH} = 1mA	0.7*Vcc		Vcc	V
$R_{I/O}$	**Pin Pull-up** SPI_SEL,SPI_SS			220		KΩ
$I_{cc\ LwPw}$	**Supply Current** in Low Power	5.0V (+/- 10%) 3.0V (+/- 10%)		240 230		µA
$I_{cc\ RunPeriph}$	**Supply Current** in RUN mode during RSA/ECC authentication			18.3		mA

6646BS – 25Sept19

Table 3-3. AC/DC Characteristics (2.7V - 5.5V range; T= -40°C to +105°C)

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
T_r	I/O Output Rise Time (HRD Mode)	C_{out}=30pF R_{pullup}=20kΩ 3V		6		ns
		C_{out}=30pF R_{pullup}=20kΩ 5V		4		ns
T_f	I/O Output Fall Time	C_{out}=30pF R_{pullup}=20kΩ 3V		3.7		ns
		C_{out}=30pF R_{pullup}=20kΩ 5V		3.2		ns

The values given in Table 3-1, Table 3-2 and Table 3-3 are targeted preliminary values that cannot be guaranteed until a full characterization of the product has been made.

3.3 Timings

3.3.1 I²C Timings

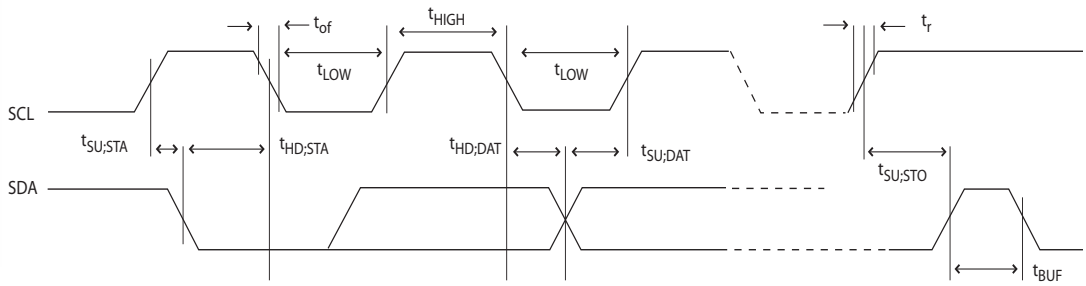
The table below describes the requirements for devices connected to the I²C Bus. The VaultIC407 I²C Interface meets or exceeds these requirements under the noted conditions.

Timing symbols refer to Figure 3-1.

Table 3-4. I²C Timings Parameters

Symbol	Parameter	Condition	Min.	Max.	Units
f_{SCL}	SCL Clock Frequency			400	kbps
$t_{SU;STA}$	Set-Up Time for a (repeated) START Condition		70		ns
$t_{HD;STA}$	Hold Time (repeated) START Condition	After this period, the first clock pulse is generated	70		ns
t_{LOW}	Low Period of the SCL Clock		490		ns
t_{HIGH}	High period of the SCL clock		130		ns
$t_{HD;DAT}$	Data hold time		40		ns
$t_{SU;DAT}$	Data setup time		50		ns
$t_{SU;STO}$	Setup time for STOP condition		70		ns
t_{BUF}	Bus free time between a STOP and a START condition		1.3		µs

Figure 3-1. I²C Timings chronograms



Note

Parameters t_{of} and t_r depend on the Host.

Note

These timings refer to Hardware communication parameters. For protocol timings, please refer to the document *VaultIC407 Technical Datasheet*.

3.3.2 SPI Timings

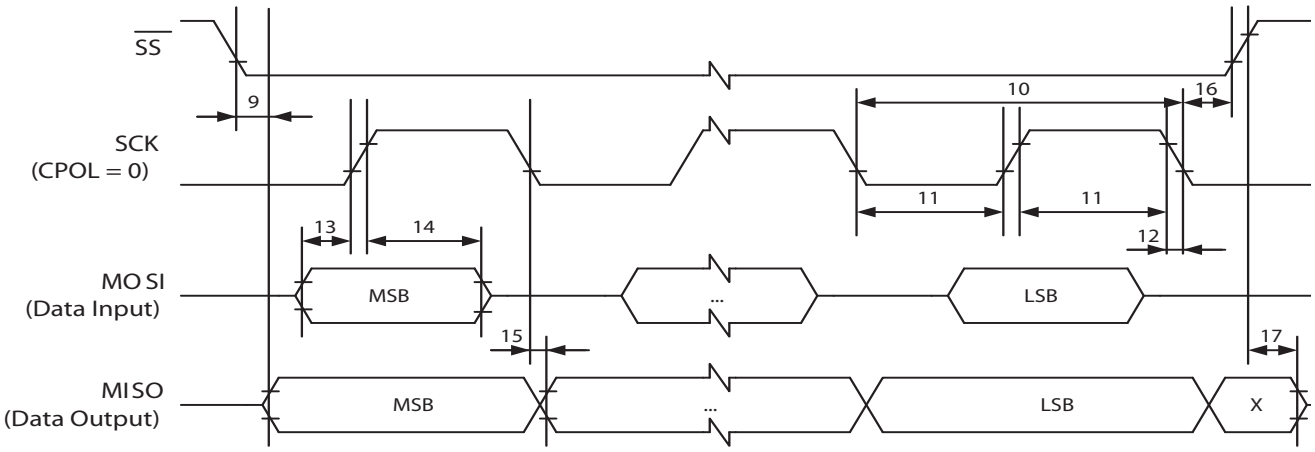
The table below describes the requirements for devices connected to the SPI. The VaultIC407 SPI meets or exceeds these requirements under the noted conditions.

Timing symbols refer to Figure 3-2.

Table 3-5. SPI Timing Parameters

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
SCK	Slave Frequency supported	C_{OUT}=10pF C_{OUT}=20pF			13	MHz
15	SCK falling to MISO Delay ($t_{SCKfalling}$)	C_{OUT}=10pF C_{OUT}=20pF			40	ns
13	MOSI Setup time before SCK rises ($t_{MOSIsetup}$)	C_{OUT}=10pF C_{OUT}=20pF	10			ns
14	MOSI Hold time after SCK rises ($t_{MOSIhold}$)	C_{OUT}=10pF C_{OUT}=20pF	10			ns
9	$\overline{SS}$ asserted to MISO time (t_{SSMISO})	C_{OUT}=10pF C_{OUT}=20pF			6	µs
10	SCK period (t_{SCK})	C_{OUT}=10pF C_{OUT}=20pF	10			ns
12	SCK Rise / Fall time ($t_{r/f}$)	C_{OUT}=10pF C_{OUT}=20pF	10			ns
11	SCK High / Low Period ($t_{highSCK}$)	C_{OUT}=10pF C_{OUT}=20pF	15			ns
16	SCK Falling to $\overline{SS}$ Rising	C_{OUT}=10pF C_{OUT}=20pF	10			ns
17	$\overline{SS}$ high to tri-state	C_{OUT}=10pF C_{OUT}=20pF	10			ns

Figure 3-2. SPI Timings chronograms



Note

These timings refer to Hardware communication parameters. For protocol timings, please refer to the document *VaultIC407 Technical Datasheet*.

3.4 Connections for Typical Application

Figure 3-3. VaultIC407 connections for **I²C** typical application

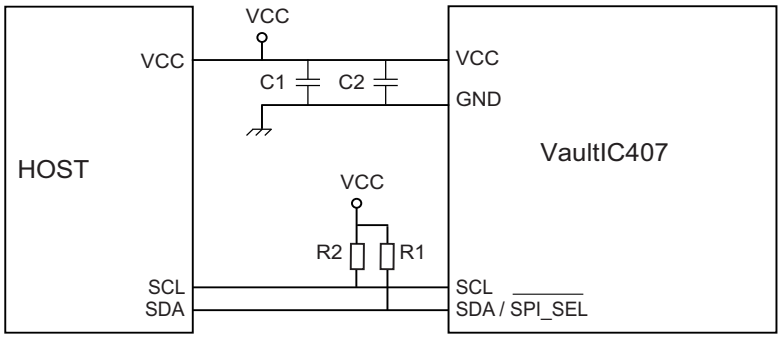


Figure 3-4. VaultIC407 connections for **SPI** typical application

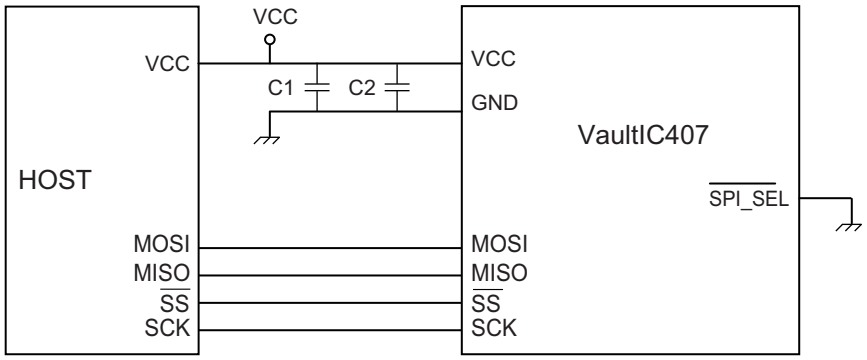


Table 3-6. External components, Bill of Materials

Configuration	Reference	Description	Typ.Value	Comment
I²C	R1, R2	Pull-Up Resistors	2.2 kΩ	Recommended
	C1	Power Supply Decoupling Capacitors	4.7 µF	Recommended
	C2	Power Supply Decoupling Capacitors	10 nF	Recommended
SPI	C1	Power Supply Decoupling Capacitors	4.7 µF	Recommended
	C2	Power Supply Decoupling Capacitors	10 nF	Recommended

3.5 Pin & Package Configuration

3.5.1 Pin Configuration

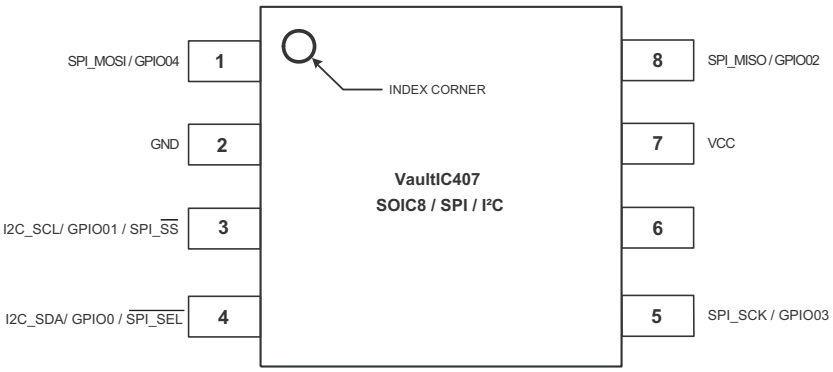
Table 3-7. Pin List Configuration

Designation	QFN20	SOIC8	Description
SPI_SCK	**16**	**5**	SPI clock
VCC	**5**	**7**	Power supply
GPIO0	**12**	**4**	General Purpose IO 0
SPI_MISO	**6**	**8**	SPI Master Input Slave Output
SPI_MOSI	**10**	**1**	SPI Master Output Slave Input
GPIO1	**14**	**3**	General Purpose IO 1
GND	**11**	**2**	Ground (reference voltage)
GPIO2	**6**	**8**	General Purpose IO 2
$\overline{\text{SPI\_SS}}$ / I2C_SCL	**14**	**3**	SPI Slave Select or I²C SCL
$\overline{\text{SPI\_SEL}}$ / I2C_SDA	**12**	**4**	SPI/I²C selection PIN or I²C SDA
GPIO3	**16**	**5**	General Purpose IO 3
GPIO4	**10**	**1**	General Purpose IO 4

Other pins are not connected (do not connect to GND).

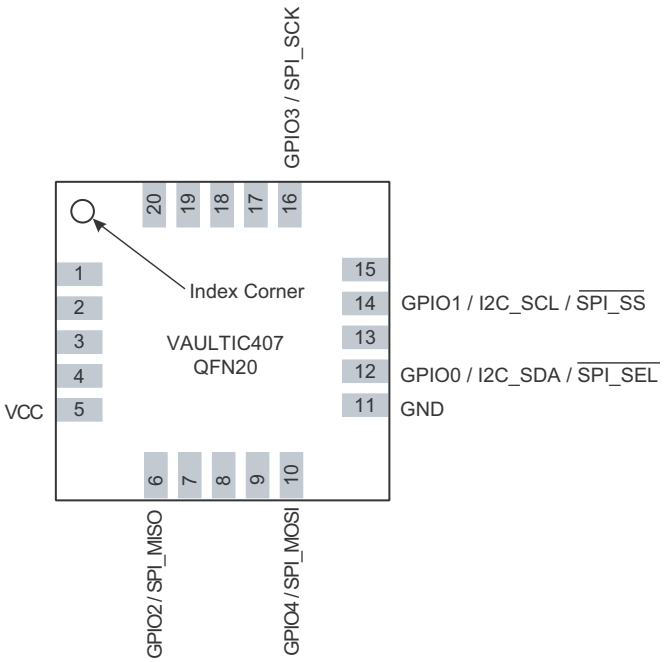
3.5.2 Pinouts for packages QFN20 and SOIC8

Figure 3-5. Pinout VaultIC407 - Package SOIC8 - SPI and I²C configurations



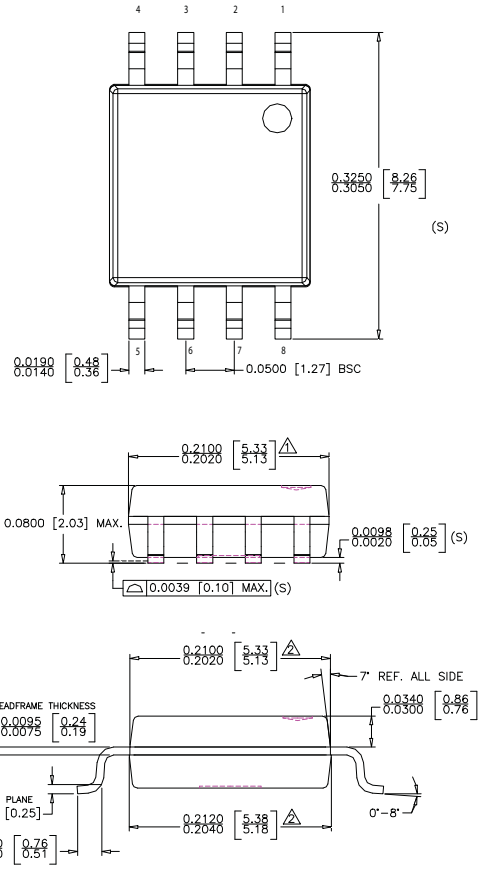
.

Figure 3-6. Pinout VaultIC407 - Package QFN20



3.5.3 Packages characteristics

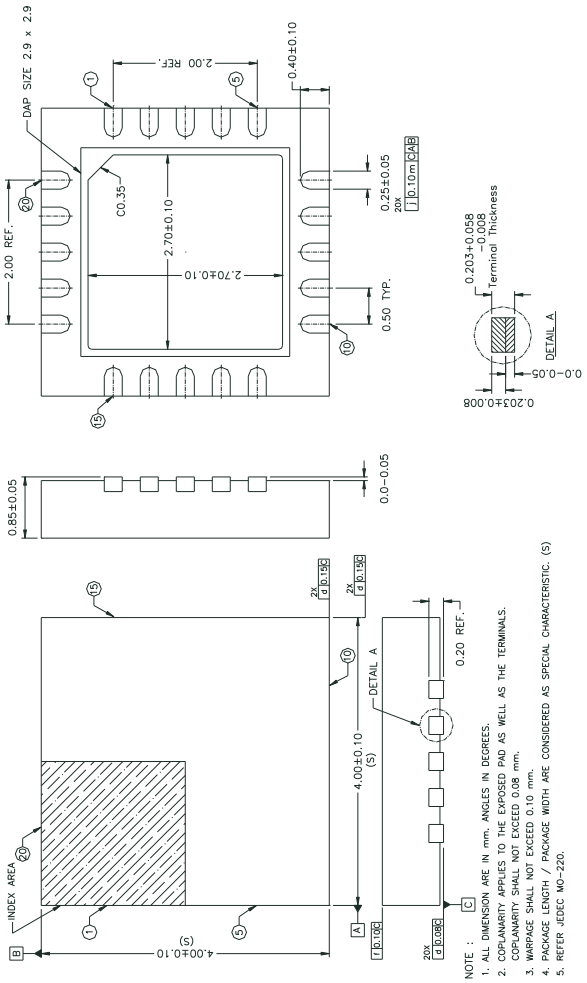
Figure 3-7. SOIC-8 package characteristics



NOTE :

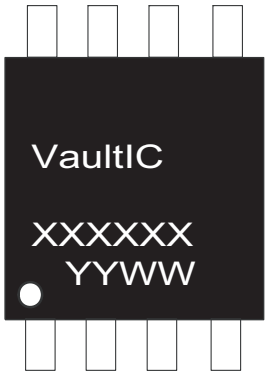
1. DOES NOT INCLUDE MOLD FLASH, PROTRUSIONS OR GATE BURRS. MOLD FLASH, PROTRUSIONS AND GATE BURRS SHALL NOT EXCEED 0.006 INCH PER SIDE.
2. DOES NOT INCLUDE INTER–LEAD FLASH OR PROTRUSIONS. INTER–LEAD FLASH AND PROTRUSIONS SHALL NOT EXCEED 0.010 INCH PER SIDE.
3. THIS PART IS COMPLIANT WITH EIAJ SPECIFICATION EDR–7320.
4. LEAD SPAN/STAND OFF HEIGHT/COPLANARITY ARE CONSIDERED AS SPECIAL CHARACTERISTIC.(S)
5. CONTROLLING DIMENSIONS IN INCHES. [mm]

Figure 3-8. QFN-20 package characteristics



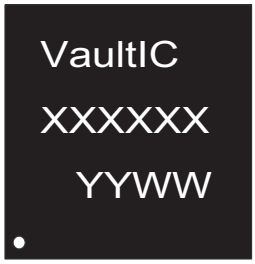
3.6 Product Marking

3.6.1 SOIC8 Package



VaultIC versionning
XXXXXX : Lot Number
YYWW : Date Code

3.6.2 QFN20Package



VaultIC versionning
XXXXXX : Lot Number
YYWW : Date Code

6646BS – 25Sept19