VaultIC405 1.2.X

Summary Datasheet

General Features

Cryptographic Services

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

Cryptographic Algorithms

- DES / 3DES
- AES 128/192/256 bits
- GCM / GMAC
- RSA® up to 4096 bits*
- DSA up to 2048 bits
- ECC up to 576 bits

Software Features

- FIPS 140-2 Identity-based authentication using password, Secure Channel Protocol (SCP02 / SCP03) or Microsoft® Smart Card Minidriver strong authentication
- Rights Management (Administrator, Approved User, Non-approved User...)
- Embedded Dynamic FAT12 File System

Memory

- File System 16 Kbytes
- Write Endurance 500 Kcycles / Data Retention 50 Years
- 7-Slot ephemeral Key Ring

Communication

- USB 2.0 Full Speed Certified, USB CCID compliant
- Slave SPI Serial Interface, SEAL SQ's Proprietary Protocol
- I²C (Two Wire Interface), SEAL SQ's Proprietary Protocol

Packages

- QFN20 (RoHS compliant) 4mm x 4mm
- SOIC8 (RoHS compliant) 5mm x 5mm

Hardware Platform

- 8-/16-bit RISC CPU
- Hardware Random Number Generator
- Hardware 3DES Crypto Accelerator (up to168-bit keys)
- Hardware AES Crypto Accelerator
- Hardware 32-bit Public Key Crypto Accelerator

Certifications / Standards

- EAL5+
- NIST CAVP
- Microsoft Smart Card Minidriver compliant
- PKCS#11

*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.
- Not available in FIPS mode

1. Overview

The VaultIC405 1.2.X 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 VaultIC405 1.2.X 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 (USB, SPI, I²C), low pin count and low power consumption are main features of the VaultIC405 1.2.X. Its embedded firmware provides advanced functions such as Identity-based authentication, large Cryptographic command set, various Public domain cryptographic algorithms, Cryptographic protocols, Secure Channel Protocols, Robust communication protocol.

1.1 Tamper resistance

SEAL SQ'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, radio emissions and other side channels attacks may give precious information on the processed data or allow the manipulation of the data. SEAL SQ'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 an SEAL SQ microcontroller.

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). Multi-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 (NIST SP 800-63) 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 microcontrollers-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 VaultIC405 1.2.X product features:

- Various **communication interfaces** including SPI (Serial Protocol Interface), I^{2}C (Two Wire Interface) or USB (Universal Serial Bus).
- **Low pin count** (Vcc, GND, and communication interface specific pins) making integration into an existing board simple. VaultIC405 1.2.X modules are available in small packages (SOIC8 or QFN20) to fit into the most size-constrained devices.
- **Low power consumption**, in order to extend battery life in portable devices and low-power systems. VaultIC405 1.2.X devices consume less than 300μA in standby mode, and only 10 to 20mA 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.
  - *Identity-based authentication* 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 DES, 3DES, AES, RSA PKCS#1 v2.1, DSA, EC-DSA, MAC using DES, 3DES or AES
  - *Cryptographic protocols* such as secret-key unilateral or mutual authentication (ISO9798-2) and public key based unilateral or mutual authentication (FIPS196).
  - *Secure Channel Protocol* using 3DES or AES.
  - *Robust communication protocol* stacked over the physical communication interfaces.
  - Starter Kit with RSA PKCS#11 and Microsoft MS-CAPI libraries.

SEAL SQ’s application note (6528C-Secure your embedded devices) presents examples of efficient and cost effective IP protection applications utilizing secure chips in various embedded systems.

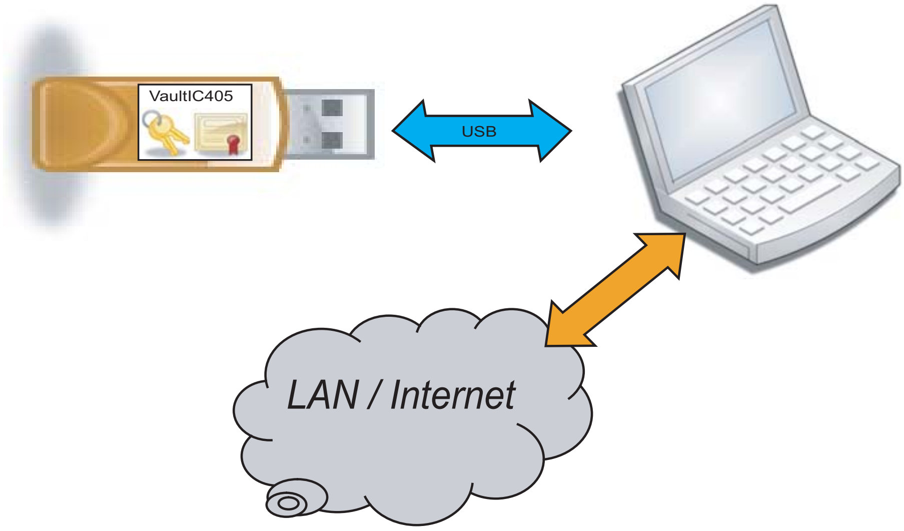
1.5 Typical application

The VaultIC405 1.2.X is a turnkey solution that combines powerful cryptographic capabilities and secure data storage. A typical application of the VaultIC405 1.2.X is the USB authentication tokens.

These tokens are carried by the employees and are mainly used for user authentication, private key and certificate storage (unlock workstations, gain access to network resources, sign and encrypt emails etc). Authentication tokens based on secure microcontrollers allow to implement high-security IT standards (EAL 5+, ISO27001, …). Public Key Infrastructures can be trusted since private keys and certificates are only handled by secure microcontrollers and can never be extracted. Convenient biometric authentication can also be implemented without privacy concerns, because fingerprint templates are handled and processed by secure controllers and are not subject to spying. Should a token be lost, it would be no issue since only the holder of the token knows the PIN code or has the right biometric attribute. No sensitive data is ever outside in the clear.

Below is described an example of a VaultIC405 1.2.X product as USB Token.

Figure 1-1. USB Token Application



For more details about this solution, please refer to the Application Note ”How to secure USB e-Token using VaultIC Security Modules?”.

1.6 Ordering Information

1.6.1 Legal

A **Non-Disclosure Agreement** must be signed with SEAL SQ.

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

1.6.2 Quotation and Volume

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

1.6.3 Part Number

Reference	Description
ATVAULTIC405-xxx-P	**xxx** : Chip “Chrono” Number* **P** = Z : QFN20 Package R : SOIC8 Package

Reference	Application	Description
ATVAULTIC-STK01-405R-x	USB Token	Starter Kit for VaultIC405 1.2.X in SOIC8 package - USB configuration + USB Dongles
ATVAULTIC-STK01-405Z-x	USB Token	Starter Kit for VaultIC405 1.2.X in QFN20 package - USB configuration + USB Dongles
ATVAULTIC-STK02-405R-x	Embedded Security	Starter Kit for VaultIC405 1.2.X in SOIC8 package - SPI/I²C configuration
ATVAULTIC-STK02-405Z-x	Embedded Security	Starter Kit for VaultIC405 1.2.X in QFN20 package - SPI/I²C configuration
ATVAULTIC-STK12-405R-x	Embedded Security	Starter Kit for VaultIC405 1.2.X in SOIC8 package - SPI/I²C configuration (SPI/I²C adapter not included)
ATVAULTIC-STK12-405Z-x	Embedded Security	Starter Kit for VaultIC405 1.2.X in QFN20 package - SPI/I²C configuration (SPI/I²C adapter not included)

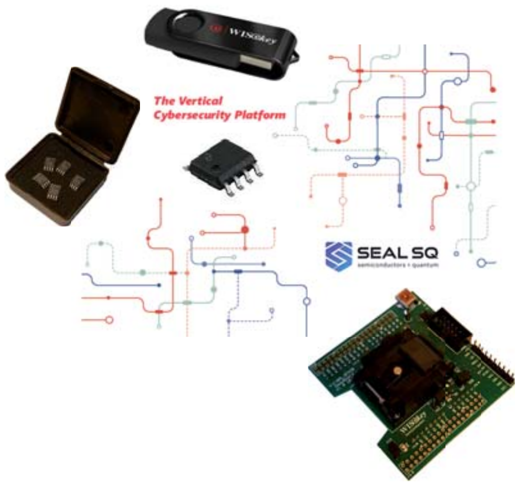
* For more details about the Chip “Chrono” Number, please contact your local SEAL SQ sales office.

1.6.4 Starter Kit

The VaultIC405 1.2.X Starter Kit provides an easy path to master the cryptographic and secure data storage features of the VaultIC405 1.2.X secure modules. The content is :

- VaultIC405 1.2.X samples with 1 dedicated test socket
- VaultIC405 1.2.X USB dongles or 1 generic USB to SPI / I²C adapter (optional)
- 1 USB FLASH drive 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 and Microsoft CSP mini-driver.

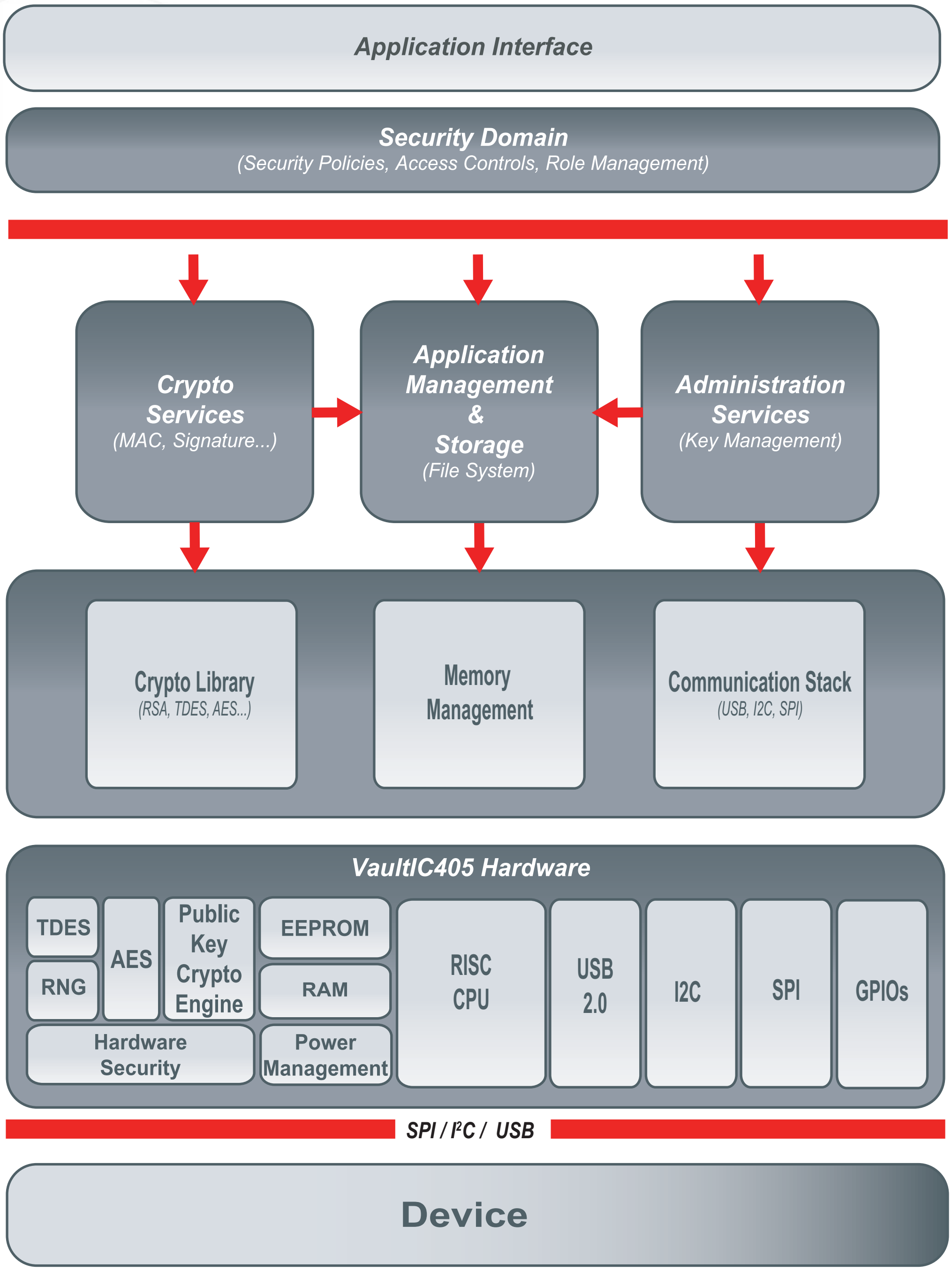
Figure 1-2. Starter Kit VaultIC405 1.2.X - Example of content



1.7 Software and Hardware Architecture

The VaultIC405 1.2.X software architecture is as shown on the diagram below.

Figure 1-3. Software and Hardware Architecture



6614HS – 17Jan23

2. Detailed Features

2.1 Communication Interfaces

The VaultIC4xx embeds the following communication interfaces:

- **USB 2.0** device full speed (up to 12 Mbps)
- **SPI**: up to 8 Mbps
- **I^{2}C** : up to 400 kbps
- **GPIOs**

2.2 Security Mechanisms

The table below summarizes the cryptographic algorithms supported by the VaultIC405 1.2.X.

Note

Please refer to the document*VaultIC Generic Datasheet* (TPR0395X- 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 • Microsoft Smartcard Minidriver • Global Platform v2.2 SCP02 using 3DES • Global Platform v2.2 SCP03 using AES
Public Key-Pair Generation	• PKCS#1.5 RSA keypair generator • ANSI X9.62 DSA keypair generator • ANSI X9.62 ECDSA keypair generator
MAC **(Message Authentication Codes)**	• ISO/IEC 9797-1 MAC algorithm 1 using 3DES with 56-bit keys • ISO/IEC 9797-1 CBC-MAC algorithm 3 using DES with 112-bit keys • NIST SP 800-38B AES CMAC • FIPS 198 HMAC with SHA-1, SHA-224, SHA-256, SHA-384 or SHA-512 • NIST SP 800-38D GMAC
Message Signature	• PKCS#1 v2.1 RSASSA PSS • PKCS#1 v2.1 RSASSA-PKCS1-v1_5 • Raw RSA X.509 with no padding • FIPS 186-3 DSA • ANSI X9.62 ECDSA over GFp and GF2m • GBCS ECDSA over GFp

Cryptographic Services	Supported Algorithms
Message Encryption	Data encryption / decryption: • DES, 2DES-EDE, 3DES-EDE and 3DES-EEE withECB, CBC, CFB or OFB chaining modes • AES • PKCS#1 v2.1 RSAES-OAEP • PKCS#1 v2.1 RSAES-PKCS1-v1.5 • Raw RSA X509 with no padding • NIST SP800-38D GCM
	Block chaining modes: • ECB • CBC • OFB • CFB • CTR
	Padding methods: • No padding • Method 1 • Method 2 • PKCS 5 • PKCS 7
HOTP - One-Time Password Generation	• OATH Has-based OTP algorithm (RFC 4226)
Message Digest	• SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512
Random Number Generation	• NIST SP 800-90 Deterministic Random Bit Generator using 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 • Generic Key Transport Scheme based on 3DES-EEE • Generic Key Transport Scheme based on 3DES-EDE

Cryptographic Services	Supported Algorithms
Key Agreement Scheme	• ANS X9.63 and FIPS SP800-56A **Static Unified** Model + BSI-TR-03111 **ECDH** over **GFp** • ANS X9.63 and FIPS SP800-56A **Static Unified** Model + BSI-TR-03111 **ECDH** over **GF2m** • ANS X9.63 and FIPS SP800-56A **One-Pass DH** Model + BSI-TR-03111 **ECDH** over **GFp** • ANS X9.63 and FIPS SP800-56A **One-Pass DH** Model + BSI-TR-03111 **ECDH** over **GF2m**
	• ANS X9.63 and FIPS SP800-56A **Static Unified** Model + ANS X9.63 **Standard DH** over **GFp** • ANS X9.63 and FIPS SP800-56A **Static Unified** Model + ANS X9.63 **Standard DH** over **GF2m** • ANS X9.63 and FIPS SP800-56A **One-Pass DH** Model + ANS X9.63 **Standard DH** over **GFp** • ANS X9.63 and FIPS SP800-56A **One-Pass DH** Model + ANS X9.63 **Standard DH** over **GF2m**
	• ANS X9.63 and FIPS SP800-56A **Static Unified** Model + ANS X9.63 **Cofactor DH** over **GFp** • ANS X9.63 and FIPS SP800-56A **Static Unified** Model + ANS X9.63 **Cofactor DH** over **GF2m** • ANS X9.63 and FIPS SP800-56A **One-Pass DH** Model + ANS X9.63 **Cofactor DH** over **GFp** • ANS X9.63 and FIPS SP800-56A **One-Pass DH** Model + ANS X9.63 **Cofactor DH** over **GF2m**
Key Derivation Function	• NIST-SP800-56A Concatenation KDF • ANS X9.63 KDF • Microsoft Smartcard Minidriver Hash KDF

Cryptographic Services	Supported Algorithms
Assurance Method for Domain Parameters Validation	• Domain Parameters should be internally obtained • Domain Parameters validated by Trusted Third Party • Domain Parameters validated by Trusted Third Party according to FIPS 186-4 • Domain Parameters selected from a set of DP trusted by Trusted Third Party • Domain Parameters validation performed by a Trusted Third Party but faulty • Domain Parameters generated by a Trusted Third Party according to FIPS 186-4 but faulty • Domain Parameters selected from a set of DP trusted by Trusted Third Party but faulty
Assurance Method for Public Key Validation	• Public Key should be internally obtained • Public Key validated by Trusted Third Party • Public Key generated by Trusted Third Party using approved methods • Public Key generated in cooperation between Trusted Third Party and the owner • Public Key generated/regenerated and pairwise test performed by Trusted Third Party • Public Key validation performed by a Trusted Third Party but faulty • Public Key generated by a Trusted Third Party using approved methods but faulty • Public Key generated in cooperation between Trusted Third Party and the owner but faulty • Public Key generated/regenerated and pairwise test performed by Trusted Third Party but faulty
Assurance Method for Private Key Validation	• Private Key should be internally obtained • Private Key generated by Trusted Third Party using approved method

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 (HBM)		4 1.5 (USB pads)	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 - MISO, MOSI, SCK, SPI_SEL, SS, GPIOs		0.7*V_{CC}		V_{CC}+0.3	V
V_{IL}	Input Low Voltage - MISO, MOSI, SCK, SPI_SEL, SS, GPIOs		-0.3		0.2*V_{CC}	V
I_{IH}	Leakage High Current - MISO, MOSI, SCK, SPI_SEL, SS, GPIOs	V_{IN} = V_{IH}	-10		10	µA
I_{IL}	Leakage Low Current - MISO, MOSI, SCK, SPI_SEL, SS, GPIOs	V_{IN} = V_{IH}	-40		10	µA
V_{OL}	Output Low Voltage - MISO, MOSI,SCK, SS, GPIOs	I_{OL} = 1mA	0		0.1*V_{CC}	V
V_{OH}	Output High Voltage - SS, MISO, MOSI, SCK, GPIOs	I_{OH} = 1mA	0.7*Vcc		Vcc	V
$R_{I/O}$	Pin Pull-up SPI_SEL,SS			220		KΩ
$I_{cc\ LowPw}$	Supply Current in Low Power	Vcc=3V			230	µA
		Vcc=5V			240	µA
$I_{cc\ Run}$	Supply Current in RUN Mode when no crypto running	Vcc=3V or 5V	4.6	5.4	6	mA

Symbol	Parameter	Condition	Min.	Typ.	Max.	Units
I_{cc} Run_Periph	Supply Current in RUN mode during RSA/ECC authentication	Vcc=3V or 5V	15.7	18.3	20	mA
$I_{cc\ DES}$	Supply Current add-on when DES running	Vcc=3V or 5V	1.3	1.5	1.7	mA
$I_{cc\ AES}$	Supply Current add-on when AES running	Vcc=3V or 5V	4.2	4.7	5.2	mA

Table 3-3. AC 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	3.1	6	9.1	ns
		C_{out}=30pF R_{pullup}=20kΩ 5V	2.3	4	5.4	ns
T_f	I/O Output Fall Time	C_{out}=30pF R_{pullup}=20kΩ 3V	2.4	3.7	7.3	ns
		C_{out}=30pF R_{pullup}=20kΩ 5V	2.1	3.2	5.3	ns

3.3 Timings

3.3.1 I²C Timings

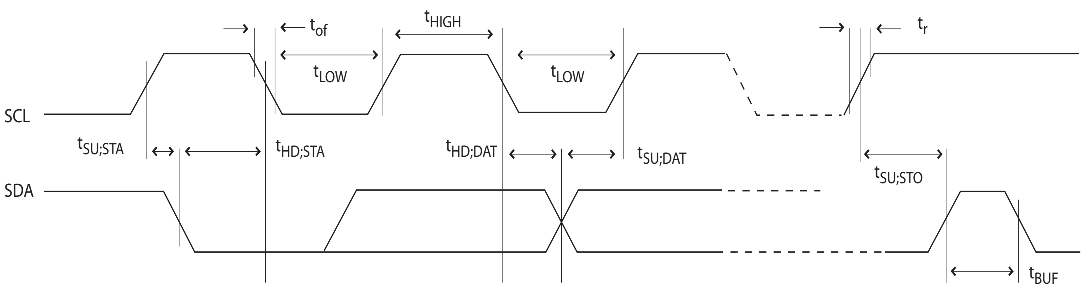
The table below describes the requirements for devices connected to the I²C Bus. The VaultIC405 1.2.X I²C Interface meets or exceeds these requirements under the noted conditions.

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.

3.3.2 SPI Timings

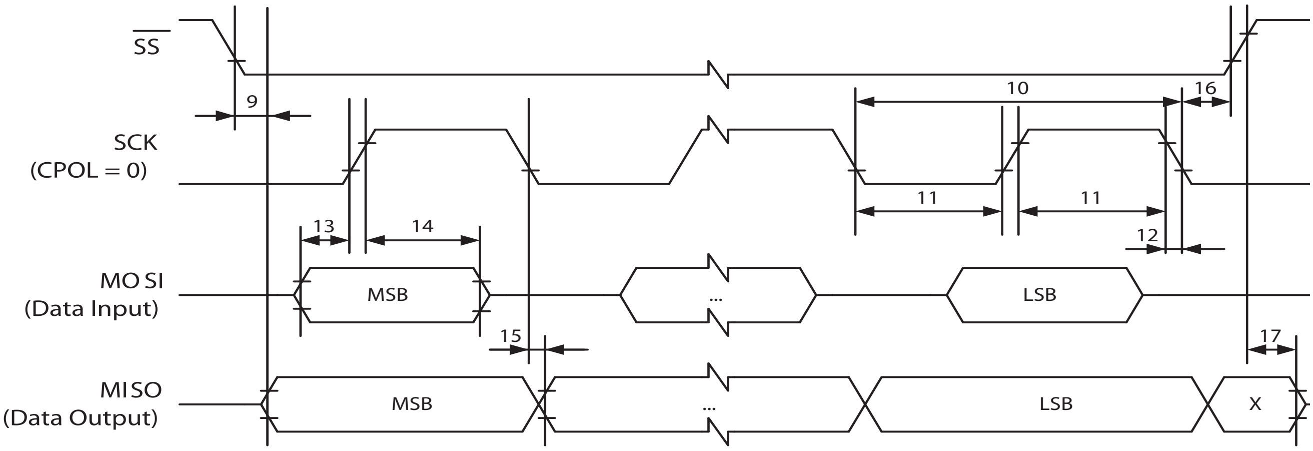
The table below describes the requirements for devices connected to the SPI. The VaultIC405 1.2.X SPI meets or exceeds these requirements under the noted conditions.

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			11	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	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.

3.4 Connections for Typical Application

Figure 3-3. VaultIC405 1.2.X connections for **USB** typical application

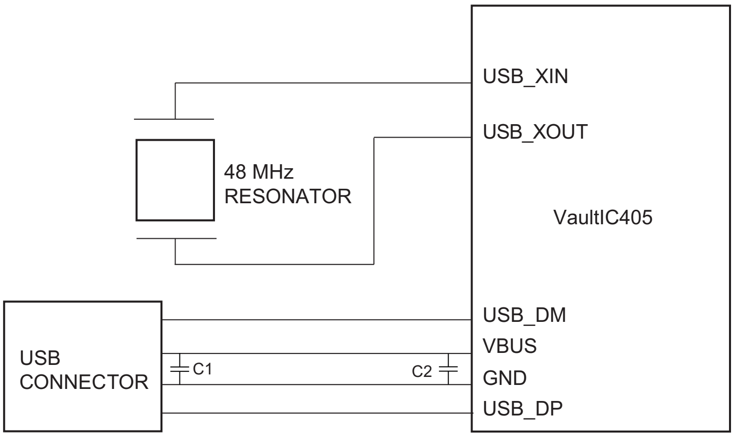


Figure 3-4. VaultIC405 1.2.X connections for **I²C** typical application

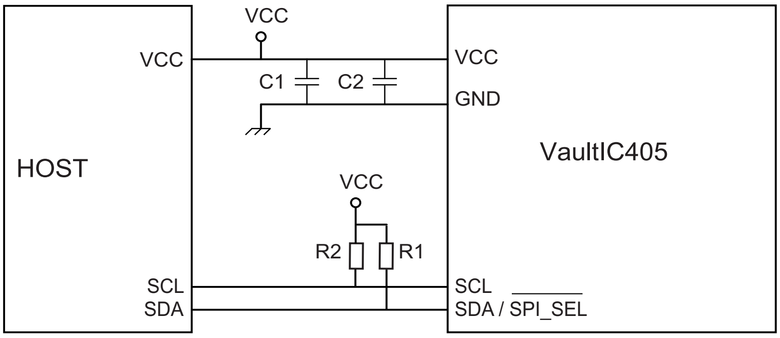


Figure 3-5. VaultIC405 1.2.X connections for **SPI** typical application

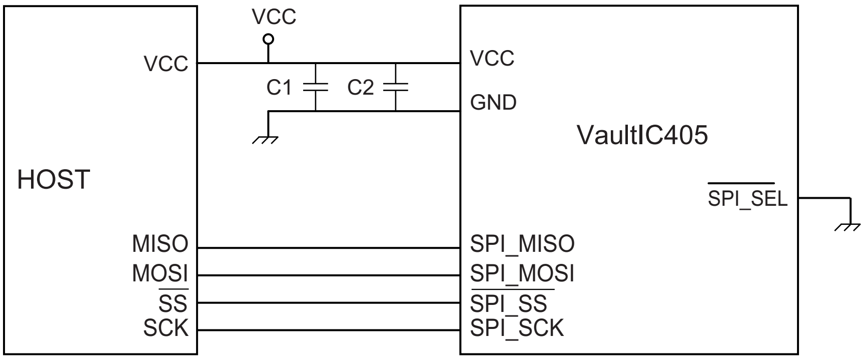


Table 3-6. External components, Bill of Materials

Configuration	Reference	Description	Typ.Value	Comment
USB		Ceramic Resonator	48MHz	Mandatory
	C1	Power Supply Decoupling Capacitor	4.7 µF	Recommended
	C2	Power Supply Decoupling Capacitor	10 nF	Recommended
I^{2}C	R1, R2	Pull-Up Resistors	2.2 kΩ	Recommended
	C1	Power Supply Decoupling Capacitor	4.7 µF	Recommended
	C2	Power Supply Decoupling Capacitor	10 nF	Recommended
SPI	C1	Power Supply Decoupling Capacitor	4.7 µF	Recommended
	C2	Power Supply Decoupling Capacitor	10 nF	Recommended

3.4.1 Internal Oscillator characteristics

The internal oscillator is optimized for a 48Mhz ceramic resonator.

Table 3-7. Internal oscillator characteristics (T= -25°C to +70°C)

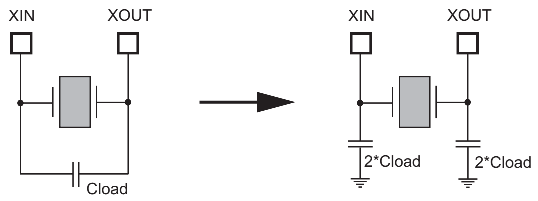
Code	Parameter	Condition	Min.	Typ.	Max.	Unit
Vdd	Supply voltage		1.4	1.8	2.0	V
ΔVdd	Supply ripple	rms value, 10kHz to 10Mhz			30	mV
Idd on	Current consumption	External capacitors: 12pF		4.8	7.1	mA
Freq	Operating frequency		40		48	MHz
Duty	Duty cycle		40		60	%
Ton	Startup time				1	ms
Pon	Drive level				500	µW
ESR	Equivalent Serie Resistance	@ 48Mhz			70	Ω
Cm	Motional capacitance	@ 48MHz	10		200	fF
Cshunt	Shunt capacitance				6.2	pF
Cload	Load capacitance	Max external capacitors: 12pF	2		6	pF
Idd stdby	Standby current consumption				1	µA

The resonator must be placed as close as possible to the VaultIC405 1.2.X chip.

The oscillator terminals shall not be used to drive other circuits.

In order to have the right resonator load capacitance, external capacitors must be connected on XIN and XOUT pins. For a given resonator, manufacturer specify a load capacitor value to add in parallel with the component. For a set of 2 caps connected between each oscillator terminal and ground, each of them should be equal to twice the specified load capacitance.

Figure 3-6. External load capacitor



SEAL SQ recommends to use the ceramic resonator CERALOCK® from *Murata* with the part number *CSTCW48M0X11Mxx-R0*. This ceramic resonator hosts built-in capacitance in a small monolithic chip type. Their electrical properties best fit the SEAL SQ specifications.

SEAL SQ recommends also CCR048.0MYC7A15T1 from TDK or NX2016HA/SA 48MHz EXS00A from NDK.

3.4.2 Building a USB Token

A **USB reference design** is available for the VaultIC405 1.2.X chip. SEAL SQ offers a complete software and hardware solution based on a full USB communication stack, an ICCD compliant library and a USB dongle as target.

Figure 3-7. USB Token schematic - Reference design

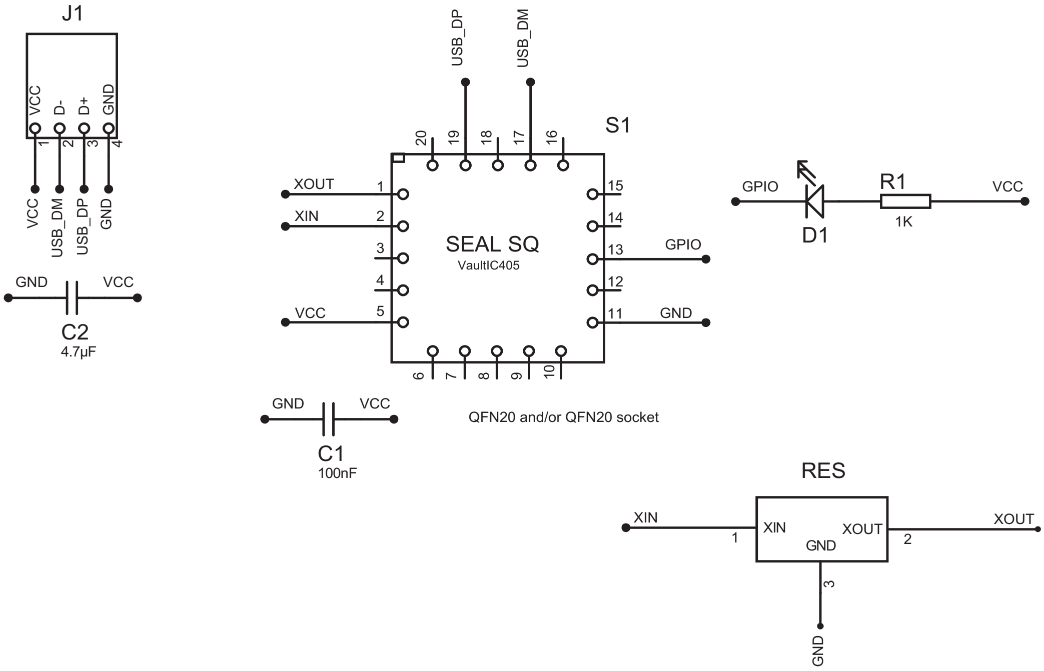


Table 3-8. Bill Of Material - Reference design

Name	Designation	Constructor Ref
S1	Microcontroller in QFN20 package	SEAL SQ VaultIC405 1.2.X
RES	48 Mhz ceramic resonator	Murata CSTCW48M0X11xx (or TDK CCR048.0MYC7A15T1 or NX2016HA 48MHz EXS00A)
J1	Plug USB Type A	Molex 48037-2000
C1	100 nF capacitance	-
C2	4.7 µF capacitance	-
R1	1K resistor	-
D1	Diode LED	KP-3216MGC

3.5 Pin & Package Configuration

3.5.1 Pin Configuration

Table 3-9. Pin List Configuration

Designation	Pin #			Description
	QFN 20	SOIC8/USB	SOIC8/SPI	
SPI_SCK	16	-	5	SPI clock
XOUT	1	6	-	Resonator Signal Input
XIN	2	7	-	Resonator Signal Output
VCC	5	8	7	Power supply
GPIO0	13	-	-	General Purpose IO 0
SPI_MISO	6	-	8	SPI Master Input Slave Output
SPI_MOSI	10	-	1	SPI Master Output Slave Input
GPIO1	12	-	-	General Purpose IO 1
GND	11	1	2	Ground (reference voltage)
GPIO2	6	-	-	General Purpose IO 2
$\overline{\text{SPI\_SS}}$ / I2C_SCL	12	2	3	SPI Slave Select or I^{2}C SCL
$\overline{\text{SPI\_SEL}}$ / I2C_SDA	13	3	4	SPI/I^{2}C selection PIN or I^{2}C SDA
GPIO3	16	-	-	General Purpose IO 3
GPIO4	10	-	-	General Purpose IO 4
USB_DM	17	4	-	USB D- differential data
USB_DP	19	5	-	USB D+ differential data

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

3.5.2 Pinouts for packages QFN20 and SOIC8

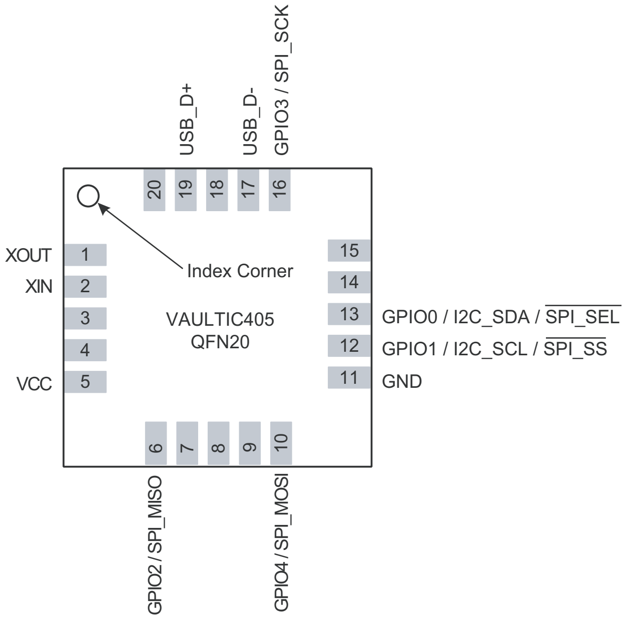


Figure 3-8. Pinout VaultIC405 1.2.X - Package QFN20

Note: Exposed pad: for better thermal dissipation, it is recommended to connect it to the GND plate.

Figure 3-9. Pinout VaultIC405 1.2.X - Package SOIC8 - USB and I²C configurations

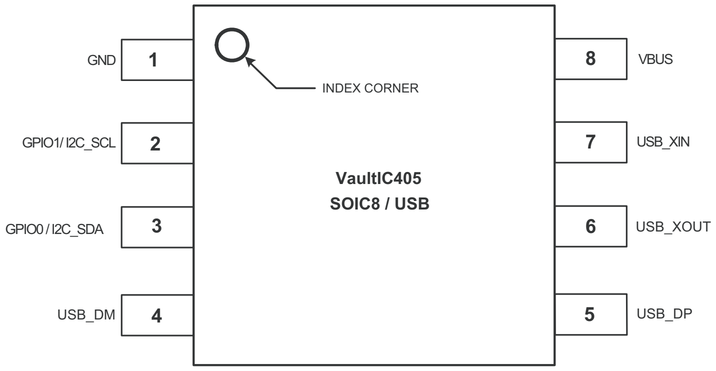
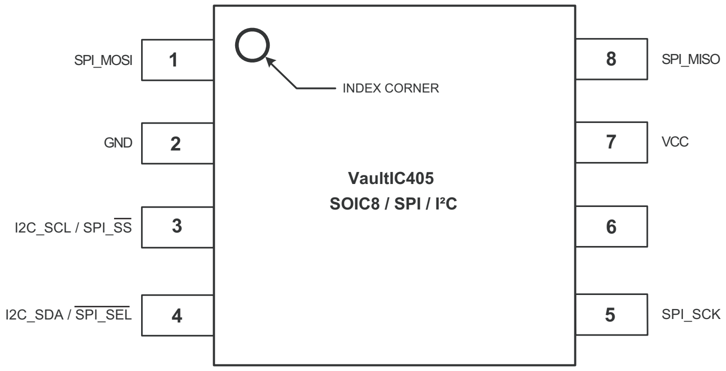
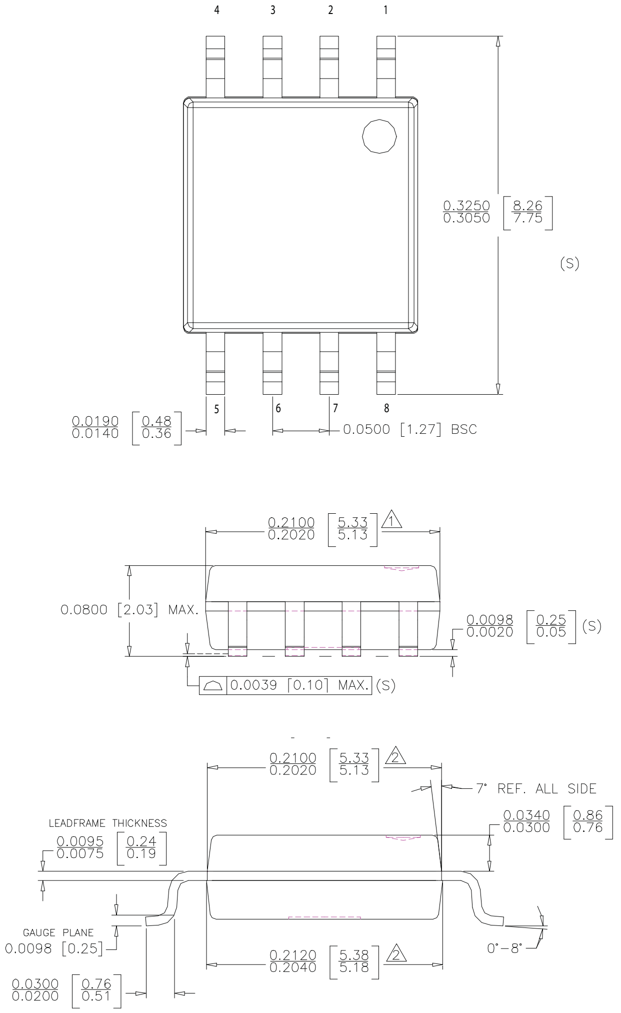


Figure 3-10. Pinout VaultIC405 1.2.X - Package SOIC8 - SPI and I²C configurations



3.5.3 Packages characteristics

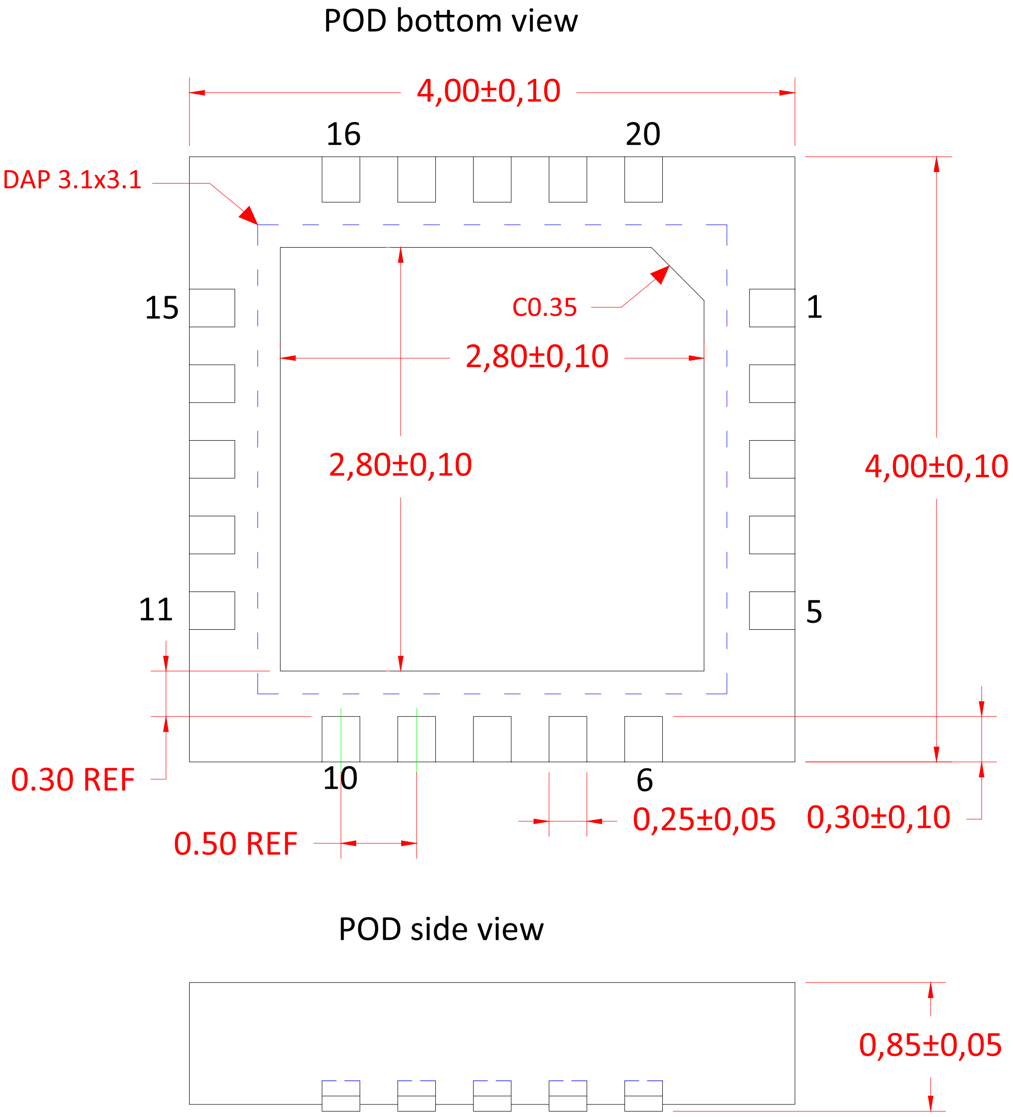
Figure 3-11. SOIC-8 package characteristics



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 3-12. QFN-20 package characteristics

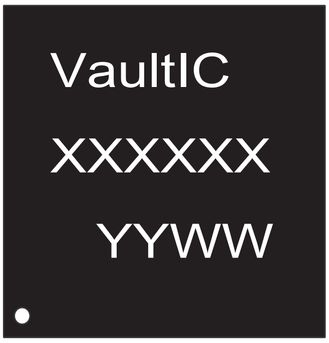


Dimensions in mm

6614HS – 17Jan23

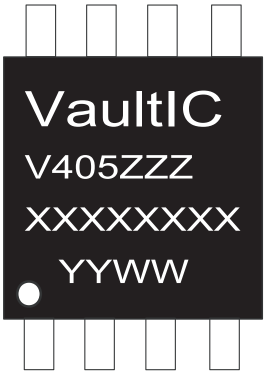
3.6 Product Marking

3.6.1 QFN20 Package



VaultIC versionning
XXXXXX : Lot Number
YYWW : Date Code

3.6.2 SOIC8 Package



VaultIC versionning
ZZZ : Internal Assembly reference
XXXXXXXX : Lot Number
YYWW : Date Code

The photographs and information contained in this document are not contractual and may be changed without notice. Brand and product names may be registered trademarks or trademarks of their respective holders.
Note: This is a summary document. A complete document will be available under NDA. For more information, please contact your local Seal SQ sales office.