VAULTIC460

Summary Datasheet

WISeKey

General Features

Cryptographic Services

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

Cryptographic Algorithms

- DES / 3DES
- AES 128/192/256 bits
- RSA® up to 4096 bits*
- DSA up to 2048 bits
- ECC up to 384 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 112Kbytes
- Write Endurance 500 Kcycles / Data Retention 20 Years
- 2ms Program + 2ms Erase

Communication

- USB 2.0 Full Speed Certified, USB CCID compliant
- High Speed Slave SPI Serial Interface, WISeKey's Proprietary Protocol
- I²C (Two Wire Interface), WISeKey's Proprietary Protocol
- ISO7816 UART using T=0 or T=1 Protocols

Packages

- QFN44 (RoHS compliant) 7mm x 7mm
- SOIC8 (RoHS compliant) 5mm x 5mm

Hardware Platform

- 8-/16-bit RISC CPU
- Hardware Random Number Generator
- Hardware 3DES Crypto Accelerator (112-bits keys)
- Hardware AES Crypto Accelerator
- Hardware 32-bit Public Key Crypto Accelerator

Certifications / Standards

- EAL4+ Ready
- FIPS 140-2 Security Level 3
- Microsoft Smart Card Minidriver compliant
- SSL support
- PKCS#11
- Microsoft MS-CAPI

*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.

6606DS – 29Sep16

1. Overview

The VaultIC460 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 VaultIC460 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, ISO7816), low pin count and low power consumption are main features of the VaultIC460. 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

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, radio emissions and other side channels attacks 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 an WISeKey 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). 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 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 VaultIC460 product features:

- Various **communication interfaces** including SPI (Serial Protocol Interface), I²C (Two Wire Interface), USB (Universal Serial Bus) or ISO7816.
- **Low pin count** (Vcc, GND, and communication interface specific pins) making integration into an existing board simple. VaultIC460 modules are available in small packages (SOIC8 or QFN44) to fit into the most size-constrained devices.
- **Low power consumption**, in order to extend battery life in portable devices and low-power systems. VaultIC460 devices consume less than 400µA 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 **112KBytes** 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 and public key based unilateral or mutual authentication .
  - *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.

WISeKey’s application note presents examples of efficient and cost effective IP protection applications utilizing secure chips in various embedded systems.

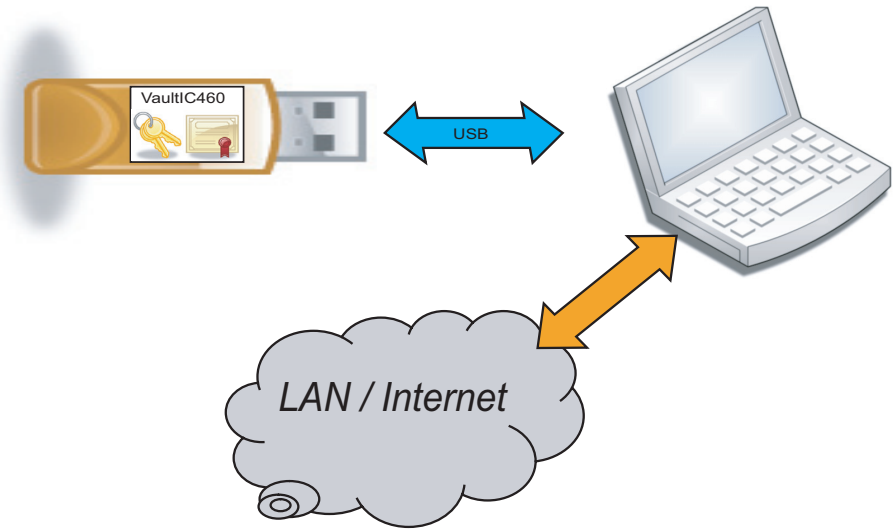
1.5 Typical application

The VaultIC460 is a turnkey solution that combines powerful cryptographic capabilities and secure data storage. A typical application of the VaultIC460 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 VaultIC460 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?* (reference TPR0451X).

1.6 Ordering Information

1.6.1 Legal

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

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 WISeKey sales office.

1.6.3 Part Number

Reference		Description
ATVAULTIC460-xxx-P		**xxx** : Chip “Chrono” Number* **P** = Z : QFN44 Package R : SOIC8 Package
Reference	**Application**	**Description**
ATVAULTIC-STK01-460R	USB Token	Starter Kit for VaultIC460 in SOIC8 package - USB configuration + USB Dongles
ATVAULTIC-STK01-460Z	USB Token	Starter Kit for VaultIC460 in QFN44 package - USB configuration + USB Dongles
ATVAULTIC-STK02-460R	Embedded Security	Starter Kit for VaultIC460 in SOIC8 package - SPI/I²C configuration
ATVAULTIC-STK02-460Z	Embedded Security	Starter Kit for VaultIC460 in QFN44 package - SPI/I²C configuration
ATVAULTIC-STK12-460R	Embedded Security	Starter Kit for VaultIC460 in SOIC8 package - SPI/I²C configuration (SPI/I²C adapter not included)
ATVAULTIC-STK12-460Z	Embedded Security	Starter Kit for VaultIC460 in QFN44 package - SPI/I²C configuration (SPI/I²C adapter not included)

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

1.6.4 Starter Kit

The VaultIC460 Starter Kit provides an easy path to master the cryptographic and secure data storage features of the VaultIC460 secure modules. The content is :

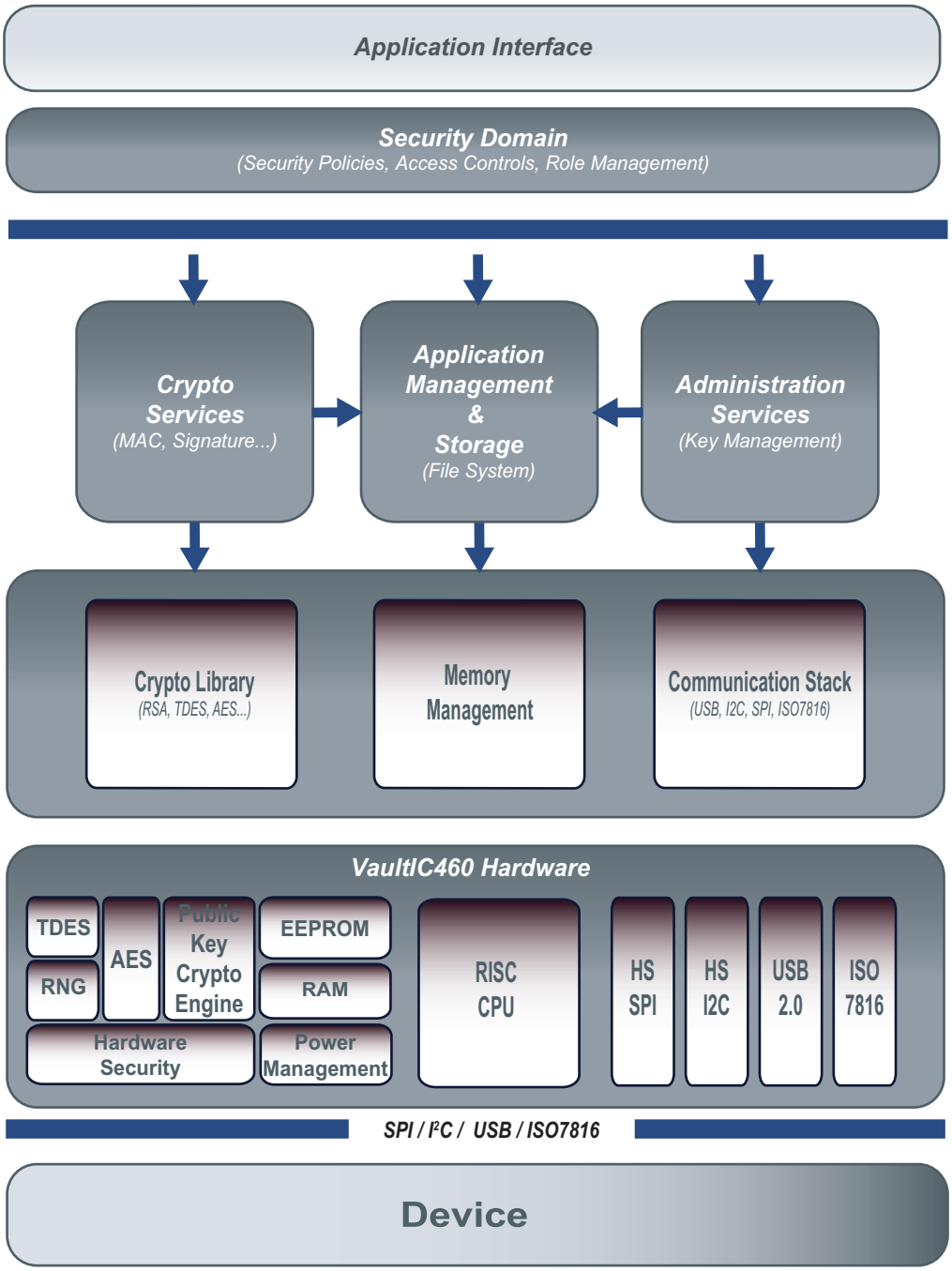
- VaultIC460 samples with 1 dedicated test socket
- VaultIC460 USB dongles or 1 generic USB to SPI / I²C adapter (optional)
- 1 CD-ROM containing a support documentation set (getting started, application notes, reference design), some demo applications to get an insight into the VaultIC4xx features, 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 VaultIC460 - Example of content

1.7 Software and Hardware Architecture

The VaultIC460 software architecture is as shown on the diagram below.

Figure 1-3. Software and Hardware Architecture



2. Detailed Features

2.1 Communication Interfaces

The VaultIC460 embeds the following communication interfaces:

- **USB 2.0** device full speed (up to 12 Mbps)
- **High Speed SPI**: up to 16 Mbps
- **I²C** : up to 400 kbps
- **ISO78186** : up to 625 kbps
- **GPIOs**

2.2 Security Mechanisms

The table below summarizes the cryptographic algorithms supported by the VaultIC460.

Please refer to the document *VaultIC Generic Datasheet* [R1] (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 Card 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 X9.31 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
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

Cryptographic Services	Supported Algorithms
Message Encryption	Data encryption / decryption: • DES, 2DES-EDE, 3DES-EDE and 3DES-EEE with ECB, 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
	Block chaining modes: • ECB • CBC • OFB • CFB
	Padding methods: • No padding • Method 1 • Method 2 • PKCS 5 • PKCS 7
HOTP - One-Time Password Generation	• OATH Hash-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

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 Virgin		20	Years
ESD	Electrostatic Discharge (HBM)		4 6 (USB pads)	kV
Lup	Latch-up		+/- 200	mA

1. At a temperature of 25°C.

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_{CC}	Supply Voltage - 5V Supply Voltage - 3V	5.0V (+/- 10%) 3.0V (+/- 10%)	4.5 2.7	5.0 3.0	5.5 3.3	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 - I/O0, SS Output Low Voltage - MISO, MOSI,SCK	I_{OL} = 1mA	0 0		0.08*V_{CC} 0.15*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
$I_{cc\ LwPw}$	Supply Current in Low Power				400	µA
$I_{cc\ RunPeriph}$	Supply Current in RUN mode during RSA/ECC authentication				20	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			100	ns
T_f	I/O Output Fall Time	C_{out}=30pF R_{pullup}=20kΩ			100	ns

3.3 Timings

3.3.1 I²C Timings

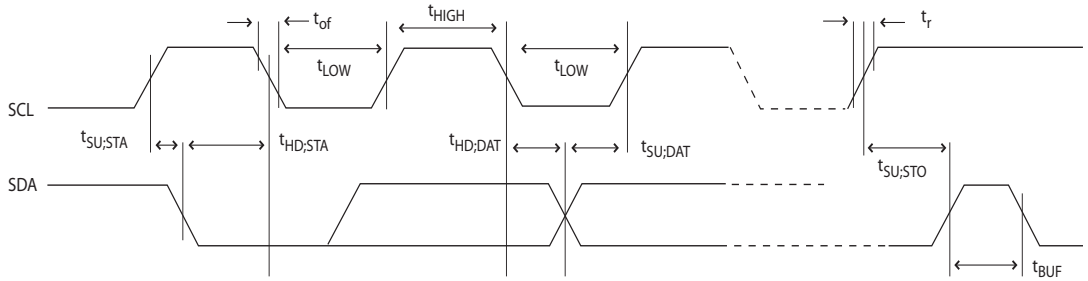
The table below describes the requirements for devices connected to the I²C Bus. The VaultIC460 I²C Interface meets or exceeds these requirements under the noted conditions.

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 *VaultIC460 Product Datasheet* (reference TPR0441X).

3.3.2 SPI Timings

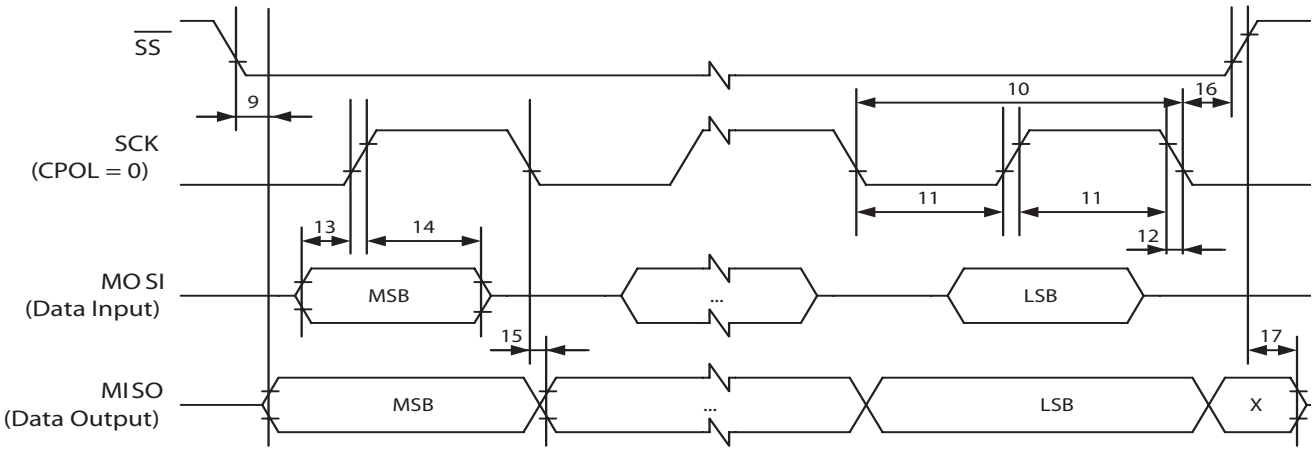
The table below describes the requirements for devices connected to the SPI. The VaultIC460 SPI meets or exceeds these requirements under the noted conditions.

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		16	20	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. For protocol timings, please refer to *VaultIC460 Product Datasheet* (reference TPR0441X).

3.4 Connections for Typical Application

Figure 3-3. VaultIC460 connections for **USB** typical application

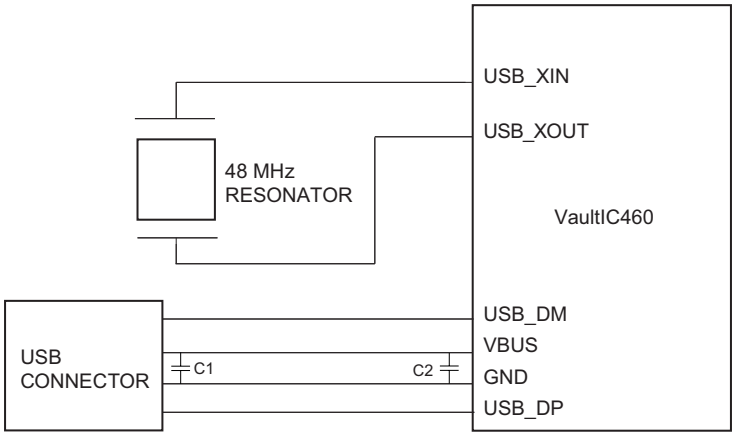


Figure 3-4. VaultIC460 connections for **I²C** typical application

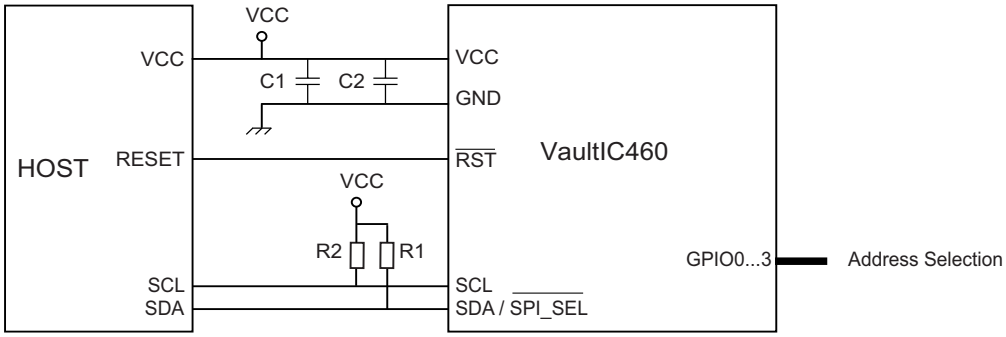


Figure 3-5. VaultIC460 connections for **SPI** typical application

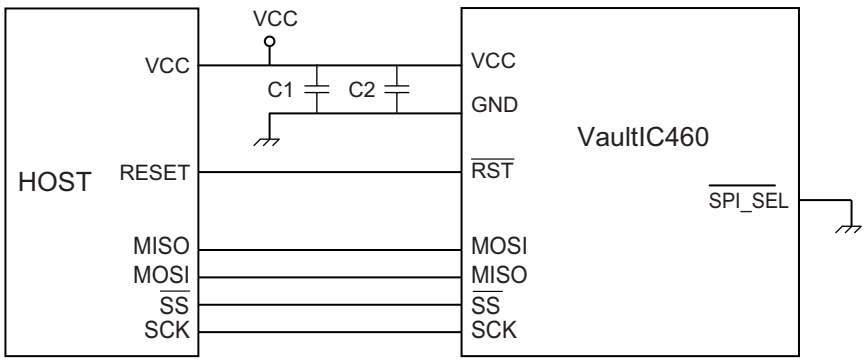


Figure 3-6. VaultIC460 connections for **ISO7816** typical application

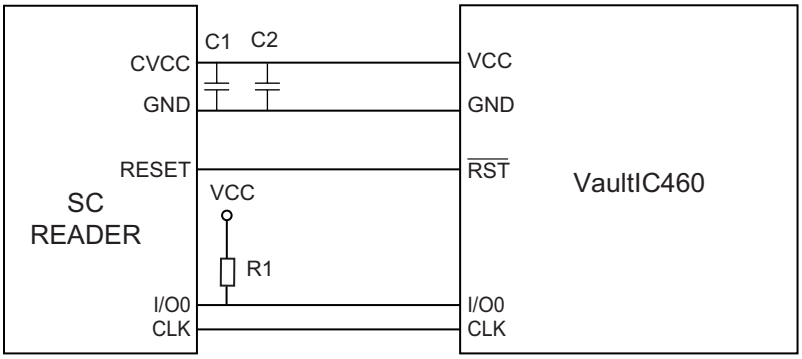


Table 3-6. External components, Bill of Materials

Configuration	Reference	Description	Typ.Value	Comment
USB		Ceramic Resonator	48MHz	Mandatory
	C1	Power Supply Decoupling Capacitors	4.7 µF	Recommended
	C2	Power Supply Decoupling Capacitors	10 nF	Recommended
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
ISO7816	R1	Pull-Up Resistor	20 kΩ	usually on reader side
	C1	Power Supply Decoupling Capacitors	4.7 µF	usually on reader side
	C2	Power Supply Decoupling Capacitors	10 nF	usually on reader side

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

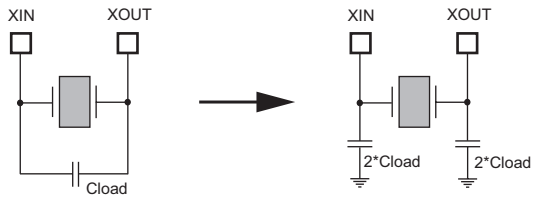
Code	Parameter	Condition	Min.	Typ.	Max.	Unit
Pon	Drive level				500	µW
ESR	Equivalent Serie Resistance	@ 48Mhz			70	Ω
Cm	Motional capacitance	@ 48MHz	10		200	fF
Cshunt	Shunt capacitance				6.2	pF
Cload	Load capacitance	Max external capacitors: 12pF	2		6	pF
Idd stdby	Standby current consumption				1	µA

The resonator must be placed as close as possible to the VaultIC460 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 3-7. External load capacitor



WISeKey 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 WISeKey specifications.

WISeKey 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 VaultIC460 chip. WISeKey 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 3-8. USB Token schematic - Reference design

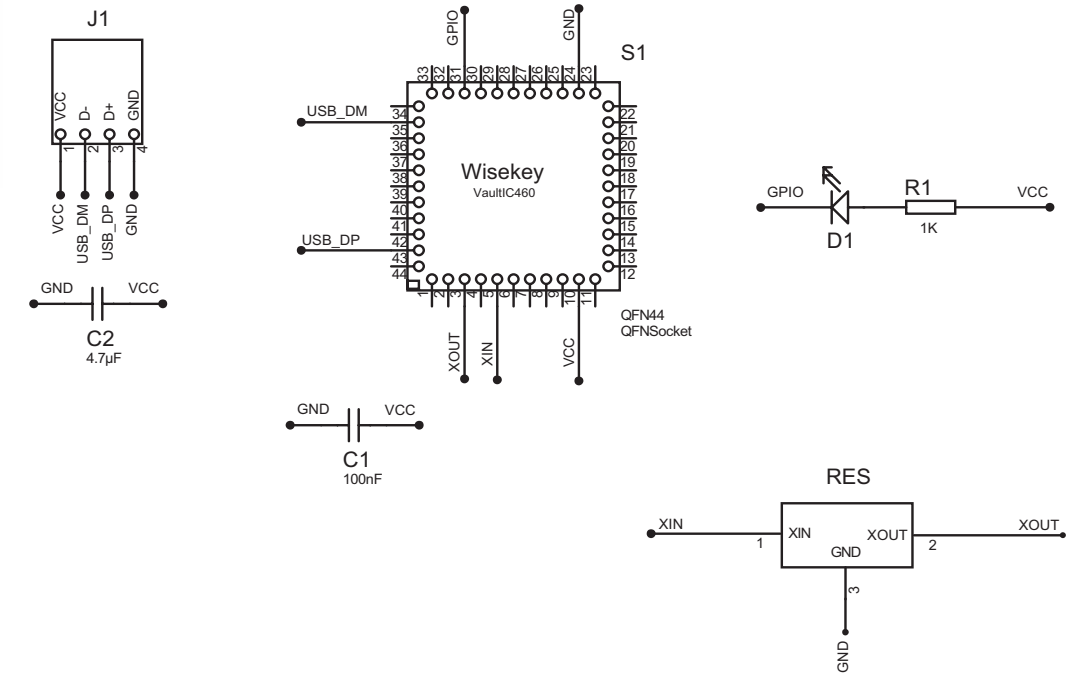


Table 3-8. Bill Of Material - Reference design

Name	Designation	Constructor Ref
S1	Microcontroller in QFN44 package	WISeKey VaultIC460
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

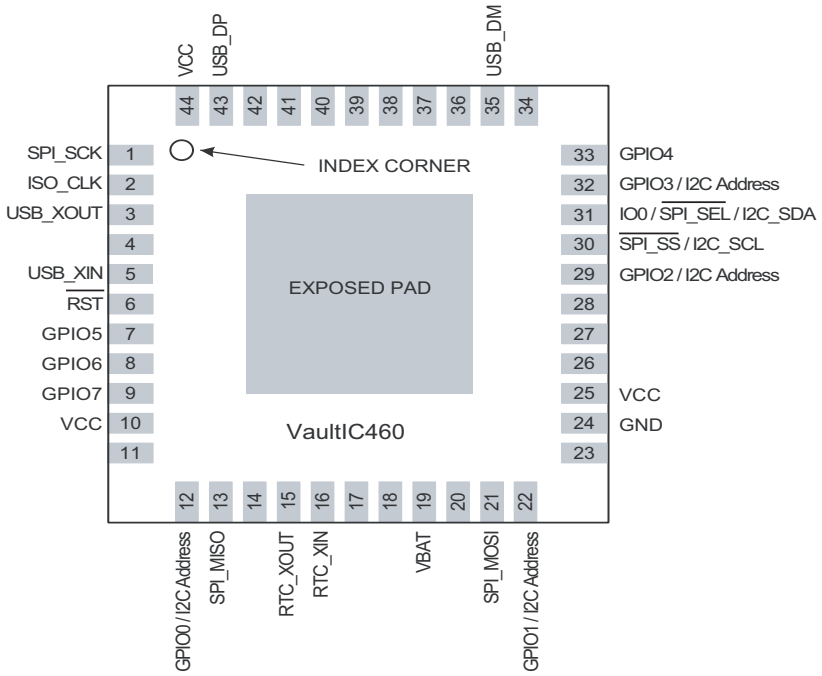
Table 3-9. Pin List Configuration

Designation	Pin #			Description
	QFN 44	SOIC8/USB	SOIC8/SPI	
SPI_SCK	1	-	5	SPI clock
ISO_CLK	2	-	-	ISO7816 clock
USB_XOUT	3	6	-	Resonator Signal Input
USB_XIN	5	7	-	Resonator Signal Output
$\overline{\text{RST}}$	6	-	6	CPU Reset
GPIO5	7	-	-	General Purpose IO 5
GPIO6	8	-	-	General Purpose IO 6
GPIO7	9	-	-	General Purpose IO 7
VCC	10,25,44	8	7	Power supply
GPIO0	12	-	-	General Purpose IO 0 / I²C Address
MISO	13	-	8	SPI Master Input Slave Output
RTC_XOUT	15	-	-	Crystal signal Input
RTC_XIN	16	-	-	Crystal signal Output
VBAT	19	-	-	Power Battery
MOSI	21	-	1	SPI Master Output Slave Input
GPIO1	22	-	-	General Purpose IO 1 / I²C Address
GND	24	1	2	Ground (reference voltage)
GPIO2	29	-	-	General Purpose IO 2 / I²C Address
$\overline{\text{SPI\_SS}}$ / I2C_SCL	30	2	3	SPI Slave Select or I²C SCL
$\overline{\text{SPI\_SEL}}$ / I2C_SDA / ISO_IO0	31	3	4	SPI/I²C selection PIN or I²C SDA or ISO7816 IO0
GPIO3	32	-	-	General Purpose IO 3 / I²C Address
GPIO4	33	-	-	General Purpose IO 4

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

3.5.2 Pinouts for packages QFN44 and SOIC8

Figure 3-9. Pinout VaultIC460 - Package QFN44



Note: The exposed pad is connected to GND pin internally. So it is recommended to connect it to GND.

Figure 3-10. Pinout VaultIC460 - Package SOIC8 - USB and I²C configurations

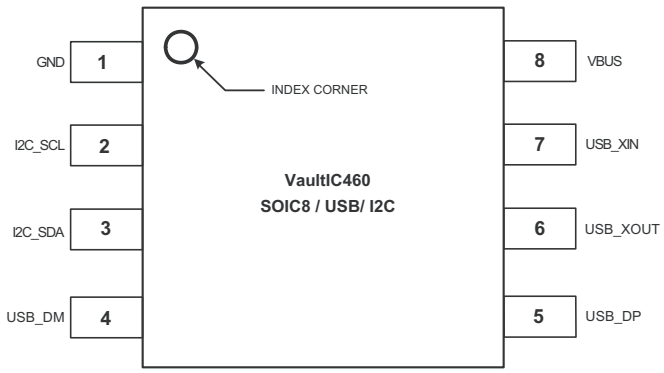
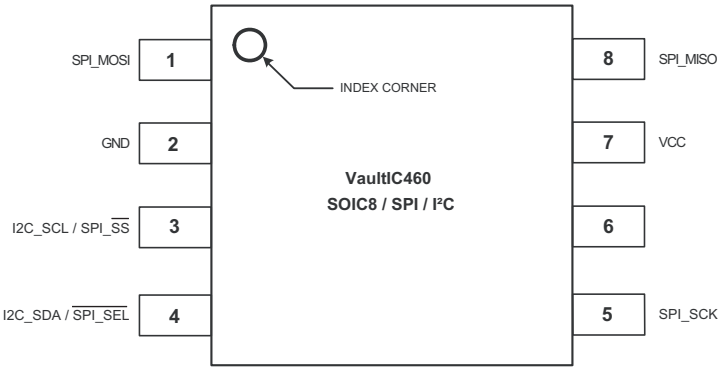
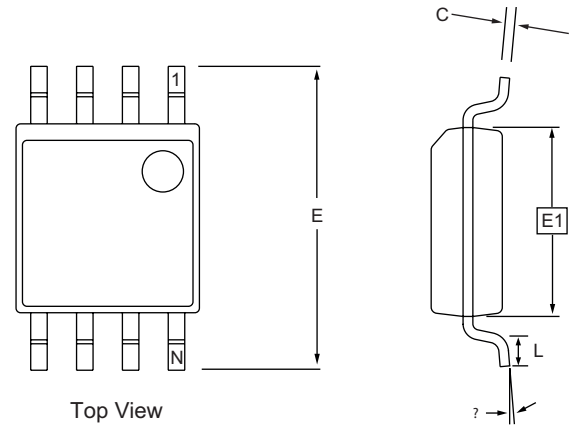


Figure 3-11. Pinout VaultIC460 - Package SOIC8 - SPI and I²C configurations



3.5.3 Packages characteristics

Figure 3-12. SOIC-8 package characteristics

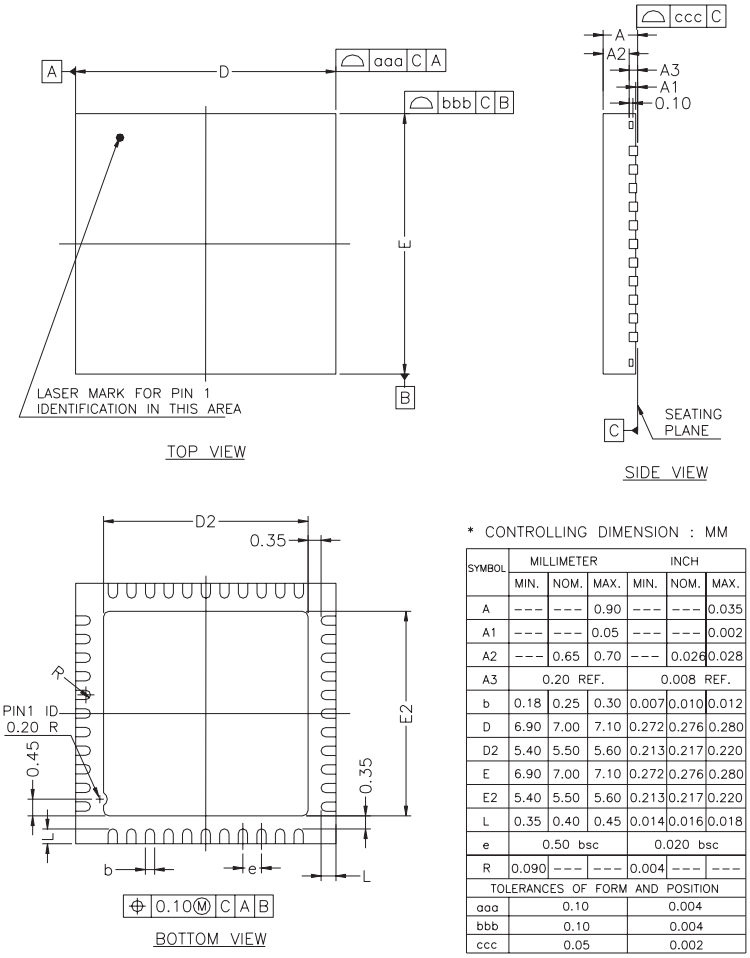


COMMON DIMENSIONS
(Unit of Measure = mm)

SYMBOL	MIN	NOM	MAX	NOTE
A	1.70		2.16	
A1	0.05		0.25	
b	0.35		0.48	5
C	0.15		0.35	5
D	5.13		5.35	
E1	5.18		5.40	2, 3
E	7.70		8.26	
L	0.51		0.85	
?	0°		8°	
e	1.27 BSC			4

Notes:
1. This drawing is for general information only; refer to EIAJ Drawing EDR-7320 for additional information.
2. Mismatch of the upper and lower dies and resin burrs are not included.
3. It is recommended that upper and lower cavities be equal. If they are different, the larger dimension shall be regarded.
4. Determines the true geometric position.
5. Values b and C apply to pb/Sn solder plated terminal.
   The standard thickness of the solder layer shall be 0.010 +0.010/-0.005 mm.

Figure 3-13. QFN-44 package characteristics



* CONTROLLING DIMENSION : MM

SYMBOL	MILLIMETER			INCH		
	MIN.	NOM.	MAX.	MIN.	NOM.	MAX.
A	---	---	0.90	---	---	0.035
A1	---	---	0.05	---	---	0.002
A2	---	0.65	0.70	---	0.026	0.028
A3	0.20 REF.			0.008 REF.		
b	0.18	0.25	0.30	0.007	0.010	0.012
D	6.90	7.00	7.10	0.272	0.276	0.280
D2	5.40	5.50	5.60	0.213	0.217	0.220
E	6.90	7.00	7.10	0.272	0.276	0.280
E2	5.40	5.50	5.60	0.213	0.217	0.220
L	0.35	0.40	0.45	0.014	0.016	0.018
e	0.50 bsc			0.020 bsc		
R	0.090	---	---	0.004	---	---
TOLERANCES OF FORM AND POSITION						
aaa	0.10			0.004		
bbb	0.10			0.004		
ccc	0.05			0.002		

NOTES :
1.ALL DIMENSIONS ARE IN MILLIMETERS.
2.PACKAGE WARPAGE MAX 0.08 mm.

3.6 Product Marking

3.6.1 QFN44 Package

zzz: VaultIC versionning
LLLLL : Lot Number
YYww : Date Code

3.6.2 SOIC8 Package

zzz: VaultIC versionning
LLLLL : Lot Number
YYww : Date Code