General Features

The ATVaultIC460 is an ASSP 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 anti-cloning, access control or hardware protection.

Cryptographic Services	Cryptographic Algorithms
• Public Key Pair Generation • Digital Signature • Encryption / Decryption • Message Digest • Key Wrapping / Unwrapping • HOTP One-Time Password Generation • True Random Number Generation	• DES / 3DES • AES 128/192/256 bits • RSA up to 4096 bits(1) • DSA up to 2048 bits • ECC up to 384 bits
Software Features	**Memory**
• FIPS 140-2 Identity-based authentication using password, Secure Channel Protocol (SCP02 / SCP03) or Microsoft® Minicard Driver strong authentication • Rights Management (Administrator, Approved User, Non-approved User...) • Embedded Dynamic FAT12 File System	• EEPROM 128 Kbytes (for user) • Write Endurance 100 Kcycles • Data Retention 10 Years • 2ms Program + 2ms Erase
Communication	**Packages**
• USB 2.0 Full Speed Certified, USB CCID compliant • High Speed Slave SPI Serial Interface, ATMEL Proprietary Protocol • I²C (Two Wire Interface), ATMEL Proprietary Protocol • ISO7816 UART using T=0 or T=1 Protocols	• 44-QFN (RoHS compliant) • 8-SOIC (RoHS compliant)
Hardware Platform	**Certifications / Standards**
• SecureAVR® 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	• EAL4+ Ready • FIPS 140-2 Security Level 3 • Microsoft CSP minidriver compliant • SSL support • PKCS#11 • Microsoft MS-CAPI

Notes: 1. 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

For more details about the alogrithms supported please refer to Table 2-1, “Supported Algorithms table,” on page 8.

VaultIC™ Family

ATVaultIC460 Technical Datasheet

TPR0441BX–SMS–09/09

Preliminary

This document is the complement to the “AT98SO Generic Datasheet” [1](TPR0395X- Available under Non-Disclosure Agreement only) for the ATVaultIC460. It only documents the values and set of features specific to this product.

1. Overview

1.1 Tampering resistance

The proven technology used in ATVaultIC460 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. More than one billion of Secure Microcontrollers addressing all these applications have been already sold by Atmel and successfully implemented in many secure systems.

Atmel'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. Atmel'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 destroy 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 Atmel secure 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 [1] 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 [3] or FIPS196 [4]), 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.

Numerous companies are now providing authentication solutions based on USB tokens. Tokens connected through USB are a convenient solution since they require no additional hardware. Atmel's turnkey USB Secure Microcontroller Solutions can help providers focus on their security model and their application without loosing too much time on tamper protection and other complex hardware security concerns.

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 ATVaultIC460 product features:

- Various **communication interfaces** including SPI (Serial Protocol Interface), I^2C (Twisted Wire Interface), USB (Universal Serial Bus) and ISO7816 SmartCard interface.
- **Low pin count** (Reset, Vcc, GND, and communication interface specific pins) making integration into an existing board simple. ATVaultIC460 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. ATVaultIC460 devices consume less than 400µA in standby mode, and only 10 to 20 mA 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 sensitive or secret data.
  - *Identity-based authentication* with user, administrator and manufacturer roles supported.
  - *Administration mode* to manage user authentication data and security features
  - *Manufacturer mode* to initialize the file system content and module parameters.
  - *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 [3] and public key based unilateral or mutual authentication [4].
  - *Secure Channel Protocol* using 3DES or AES.
  - *Robust communication protocol* stacked over the physical communication interfaces.

– *Starter Kit* with RSA® PKCS#11 [5] and Microsoft® MS-CAPI [6] libraries.

Atmel's application note [7] presents examples of efficient and cost effective IP protection applications utilizing secure chips in various embedded systems.

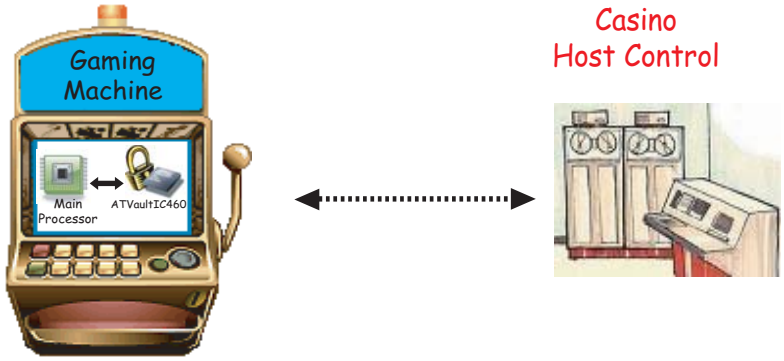
1.5 Typical application

The ATVaultIC460 is a turnkey solution that combines powerful cryptographic capabilities and secure data storage. A typical application of the ATVaultIC460 is Video Slot Gaming Machines.

Fraud, theft and embezzelment are the big fears of casinos so that they look for security inside their gaming machines.

An ATVaultIC460 linked to the main processor of the machine allows authentication of the host controller (casino) and of the slot machine. Moreover physical protection of the sensitive code/data, data encryption, secure communication channel, data integrity checking are other security features provided by the ATVaultIC460.

Figure 1-1. Gaming Application



For more details about the solution, please refer to the Application Note "How to secure Video Slot Gaming Machines using VaultIC™ Security Modules?"[7].

1.6 Ordering Information

1.6.1 Legal

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

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

1.6.2 Quotation and Volume

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

1.6.3 Part Number

Reference	Description
ATVaultIC460-Z	ATVaultIC460 chip in QFN44 package
ATVaultIC460-R	ATVaultIC460 chip in SOIC8 package (USB, SPI/I²C or ISO7816 configuration)
ATVaultIC-STK02-460Z	Starter Kit for ATVaultIC460 in QFN44 package
ATVaultIC-STK02-460R	Starter Kit for ATVaultIC460 in SOIC8 package

1.6.4 Starter Kit

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

- ATVaultIC460 samples with 1 dedicated test socket
- ATVaultIC460 USB dongles
- 1 CD-ROM containing a support documentation set (getting started, application notes, reference design), some demo applications to get an insight into the ATVaultIC features, the ”AT98 Manager” tool to design the file system and to personalize samples, a hardware independent cryptographic API with source code.

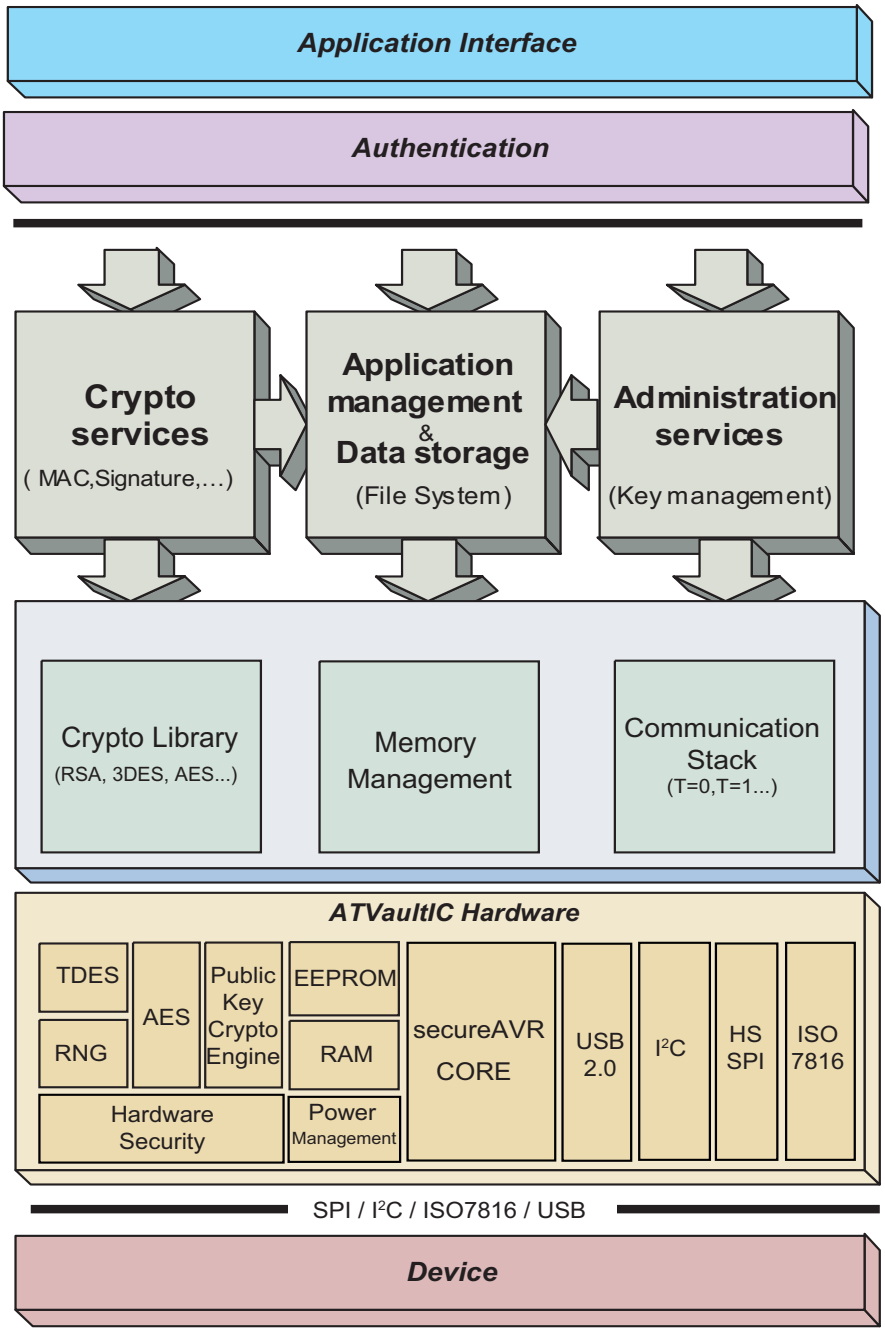
1.6.5 Demo Kit

TBD

1.7 Software and Hardware Architecture

The ATVaultIC460 software architecture is as exposed on the diagram below.

Figure 1-2. Software and Hardware Architecture



2. Detailed Features

2.1 Communication Interfaces

The ATVaultIC460 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
- **ISO7816** : up to 625 kbps

2.2 Security Mechanisms

The table below summarizes the cryptographic algorithms, and their identifiers, supported by the ATVaultIC460.

Table 2-1. Supported Algorithms table

Cryptographic Services	Supported Algorithms	Algo Identifiers
Strong Authentication	• Generic: ISO/IEC 9798-2 / FIPS 196 unilateral authentication protocol ISO/IEC 9798-2 mutual authentication protocol • Password authentication	-
	• Global Platform v2.2 Secure Channel 02 (SCP02) using 3DES • Global Platform v2.2 Secure Channel 03 (SCP03) using AES	-
	• Microsoft Card Minidriver	-
Public Key-Pair Generation	• RSA key-pair generation • Elliptic Curves key-pair generation • DSA key-pair generation	• KGEN_RSA • KGEN_ECDSA • KGEN_DSA
CMAC **(Cipher-based Message Authentication Codes)**	• ISO/IEC 9797-1 CBC-MAC algorithm 1 using 3DES with 112-bit keys • ISO/IEC 9797-1 CBC-MAC algorithm 3 using DES with 56-bit keys • NIST SP 800-38B AES CMAC	• ALG_MAC_ISO9797_ALG1_3DES_EDE • ALG_MAC_ISO9797_ALG3_DES • ALG_CMAC_AES
HMAC **(Hash-based Message Authentication Codes)**	• FIPS 198 HMAC with SHA-1 or SHA-256	• ALG_HMAC
Message Signature	• PKCS#1 v2.1 RSASSA PSS • PKCS#1 v2.1 RSASSA-PKCS1-v1_5 • FIPS 186-2 ECDSA • FIPS 186-2 DSA	• ALG_RSASSA_PKCS_PSS • ALG_RSASSA_PKCS • ALG_ECDSA • ALG_DSA

Cryptographic Services	Supported Algorithms	Algo Identifiers
Message Encryption	Block Ciphering: • DES • 3DES-EDE • 3DES-EEE • AES	 • ALG_DES • ALG_3DES_EDE • ALG_3DES_EEE • ALG_AES
	Block chaining modes: • ECB • CBC • OFB • CFB	 • CHA_ECB • CHA_CBC • CHA_OFB • CHA_CFB
	Padding methods: • No padding • Method 1 • Method 2 • PKCS 5 • PKCS 7	 • PAD_NONE • PAD_METHOD_1 • PAD_METHOD_2 • PAD_PKCS5 • PAD_PKCS7
	Encryption: • PKCS#1 v2.1 RSAES-OAEP • PKCS#1 v2.1 RSAES-PKCS1-v1.5 • Raw RSA X509 with no padding	 • ALG_RSAES_PKCS_OAEP • ALG_RSAES_PKCS • ALG_RSAES_X509
HOTP - One-Time Password Generation	• FIPS 198 HMAC algorithm with SHA1 digest	• ALG_HOTP
Message Digest	• SHA-1 • SHA-224 • SHA-256	• ALG_SHA1 • ALG_SHA224 • ALG_SHA256
Random Number Generation	• FIPS 140-2 LVL3 using 3DES	-

3. Product Characteristics

3.1 Command Timings (T=25°C)

Caution **The table below includes only the ATVaultIC460 internal process. Communication protocol overhead and device-side process are excluded.**

Table 3-1. Command Timings table

Command (or batch of commands)	Context	Min.	Typ.	Max.	Unit
Encryption / Decryption	DES-ECB, 258 bytes data		TBD		ms
Encryption / Decryption	3DES-ECB, 258 bytes data		TBD		ms
Encryption / Decryption	AES		TBD		ms
Encryption	RSAES-OAEP 1024-bit RSA key, public exp 2^{16+1}		TBD		ms
Encryption	RSAES-OAEP 2048-bit RSA key, public exp 2^{16+1}		TBD		ms
Encryption	RSAES-OAEP 4096-bit RSA key, public exp 2^{16+1}		TBD		ms
Decryption	RSAES-OAEP 1024-bit RSA key, public exp 2^{16+1}		TBD		ms
Decryption	RSAES-OAEP 2048-bit RSA key, public exp 2^{16+1}		TBD		ms
Decryption	RSAES-OAEP 4096-bit RSA key, public exp 2^{16+1}		TBD		ms
Decryption	RSAES-OAEP 4096-bit RSA CRT key, public exp 2^{16+1}		TBD		ms
Signature / Verification	MAC DES algo 3 padding M2, 258 bytes data		TBD		ms
Signature / Verification	MAC DES algo 1 padding M2, 258 bytes data		TBD		ms
Signature / Verification	RSASSA-PSS 1024-bit RSA key, public exp 2^{16+1}		TBD		ms
Signature / Verification	RSASSA-PSS 2048-bit RSA key, public exp 2^{16+1}		TBD		ms
Signature / Verification	RSASSA-PSS 4096-bit RSA key, public exp 2^{16+1}		TBD		ms
Signature / Verification	RSASSA-PKCS-v1_5 1024-bit RSA key, public exp 2^{16+1}		TBD		ms
Signature / Verification	RSASSA-PKCS-v1_5 2048-bit RSA key, public exp 2^{16+1}		TBD		ms
Signature / Verification	RSASSA-PKCS-v1_5 4096-bit RSA key, public exp 2^{16+1}		TBD		ms
Signature / Verification	DSA		TBD		ms
Signature / Verification	ECDSA		TBD		ms
Signature / Generation	MAC DES algo 3 padding M2, 258 bytes data		TBD		ms
Signature / Generation	MAC DES algo 1 padding M2, 258 bytes data		TBD		ms
Signature / Generation	RSASSA-PSS 1024-bit RSA key, public exp 2^{16+1}		TBD		ms
Signature / Generation	RSASSA-PSS 2048-bit RSA key, public exp 2^{16+1}		TBD		ms
Signature / Generation	RSASSA-PSS 4096-bit RSA key, public exp 2^{16+1}		TBD		ms
Signature / Generation	RSASSA-PKCS-v1_5 1024-bit RSA key, public exp 2^{16+1}		TBD		ms
Signature / Generation	RSASSA-PKCS-v1_5 2048-bit RSA key, public exp 2^{16+1}		TBD		ms

Command (or batch of commands)	Context	Min.	Typ.	Max.	Unit
Signature / Generation	RSASSA-PKCS-v1_5 4096-bit RSA key, public exp 2^{16+1}		TBD		ms
Signature / Generation	DSA		TBD		ms
Signature / Generation	ECDSA		TBD		ms
Key Generation	ECC		TBD		ms
Key Generation	RSA 1024-bits, public exp 2^{16+1}	TBD	TBD	TBD	ms
Key Generation	RSA 2048-bits, public exp 2^{16+1}	TBD	TBD	TBD	ms
Key Generation	RSA 4096-bits, public exp 2^{16+1}	TBD	TBD	TBD	ms
Key Generation	DSA	TBD	TBD	TBD	ms

3.2 Maximum Ratings

Table 3-2. Absolute Maximum Ratings[1]

Operating Temperature	-25°C to +85°C
Supply Voltage V_{cc}	-0.3V to +7.5V
Input Voltage V_{in}	V_{ss}-0.3V to V_{cc}+0.3V
Maximum Operating Voltage	7.5V
DC Current V_{CC} and GND Pins	TBD

Notes: 1. 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.

3.3 AC/DC Characteristics (2.7V - 5.5V range; T= -25°C to +85°C)

Table 3-3. AC/DC Characteristics (2.7V - 5.50V range; T= -25°C to +85°C)

Symbol	Parameter	Condition	Min.	Typ.	Max.	Unit
V_{CC}	Supply Voltage	3.0V (+/-10%) 5.0V (+/-10%)	2.7 4.5	3.0 5.0	3.3 5.5	V
V_{bat}	Power Battery		2.2	3	3.5	
V_{MAX}	Voltage Monitor: high level detection		5.5			V
V_{MIN}	Voltage Monitor: low level detection	3.0V, 5.0V			2.7	V
T_{MAX}	Temperature Monitor: high level detection		85			°C
T_{MIN}	Temperature Monitor: low level detection				-25	°C

Symbol	Parameter	Condition	Min.	Typ.	Max.	Unit
V_{IH}	Input High Voltage - I/O0,CLK,RST, MISO,MOSI,SCK, SPI_SEL, SS		0.7*V_{CC}		V_{CC}+0.3	V
V_{IL}	Input Low Voltage- - I/O0,CLK,RST, MISO,MOSI,SCK, SPI_SEL, SS		V_{SS}-0.3		0.2*V_{CC}	V
I_{IH}	Leakage High Current- I/O0,CLK,RST, MISO,MOSI,SCK, SPI_SEL, SS	V_{IN} = V_{IH}	-10		10	µA
I_{IL}	Leakage Low Current - I/O0,CLK,RST, MISO,MOSI,SCK, SPI_SEL, SS	V_{IN} = V_{IL}	-40		10	µA
V_{OL}	Output Low Voltage - I/O 0,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 - I/O 0,SS, MISO, MOSI, SCK	I_{OH} = 1mA	0.7*V_{CC}		V_{CC}	V
$R_{I/O}$	Pin Pull-up I/O0, RST,SPI_SEL,SS			220		KOhm
f_{SCK}	SPI Clock (Input)	Duty cycle=40% to 60%	TBD	20	TBD	MHz
T_r	I/O Output Rise Time (HRD Mode)	C_{out}=30pF R_{pullup}=20kOhm			1	µs
T_f	I/O Output Fall Time	C_{out}=30pF R_{pullup}=20kOhm			1	µs
I_{cc}	Typical Current at 25°C	- Chip in low power mode: • 400µA when external clock supplied • 400µA when no external clock is supplied (CLK signal in high state) - Chip awaken, no crypto running: • 6mA when external clock supplied • 10mA when no external clock is supplied (CLK signal in high state) - Additional consumption during RSA/ECC authentication: • 4mA when external clock supplied • 20mA when no external clock is supplied (CLK signal in high state) - Additional consumption during DES computations: • 4mA when external clock supplied • 10mA when no external clock is supplied (CLK signal in high state)				

3.4 Timings

3.4.1 I²C Timings

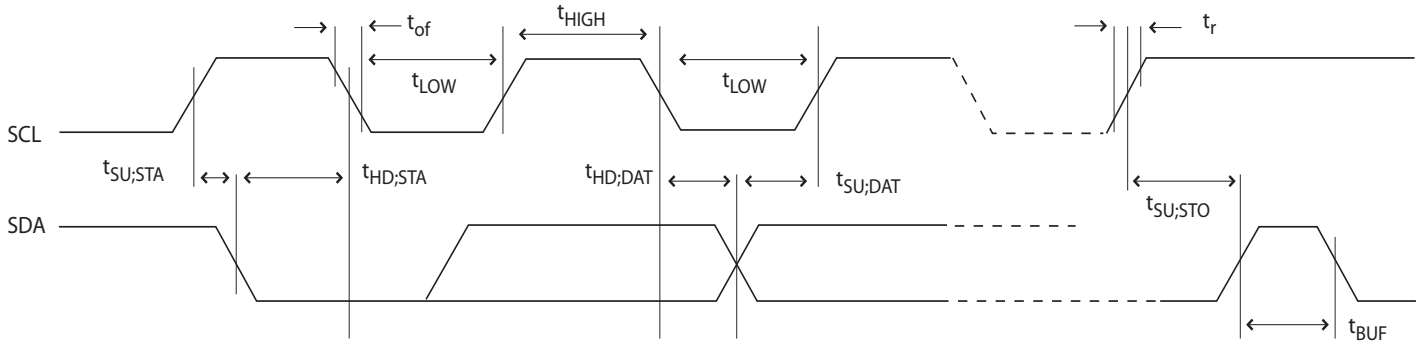
The table below describes the requirements for devices connected to the I²C Bus. The ATVaultIC460 I²C Interface meets or exceeds these requirements under the noted conditions.

Timing symbols refer to Figure 3-1.

Table 3-4. I²C Requirements

Symbol	Parameter	Condition	Min	Max	Unit
t_r	Rise Time for both SDA and SCL		TBD	TBD	ns
t_{of}	Output Fall Time from V_{IHmin} to V_{ILmax}		TBD	TBD	ns
f_{SCL}	SCL Clock Frequency		TBD	100	kHz
$t_{HD;STA}$	Hold Time (repeated) START Condition		TBD	TBD	µs
t_{LOW}	Low Period of the SCL Clock		TBD	TBD	µs
t_{HIGH}	High period of the SCL clock		TBD	TBD	µs
$t_{SU;STA}$	Set-up time for a repeated START condition		TBD	TBD	µs
$t_{HD;DAT}$	Data hold time		TBD	TBD	µs
$t_{SU;DAT}$	Data setup time		TBD	TBD	ns
$t_{SU;STO}$	Setup time for STOP condition		TBD	TBD	µs
t_{BUF}	Bus free time between a STOP and START condition		TBD	TBD	µs

Figure 3-1. I²C Timings



3.4.2 SPI Timings

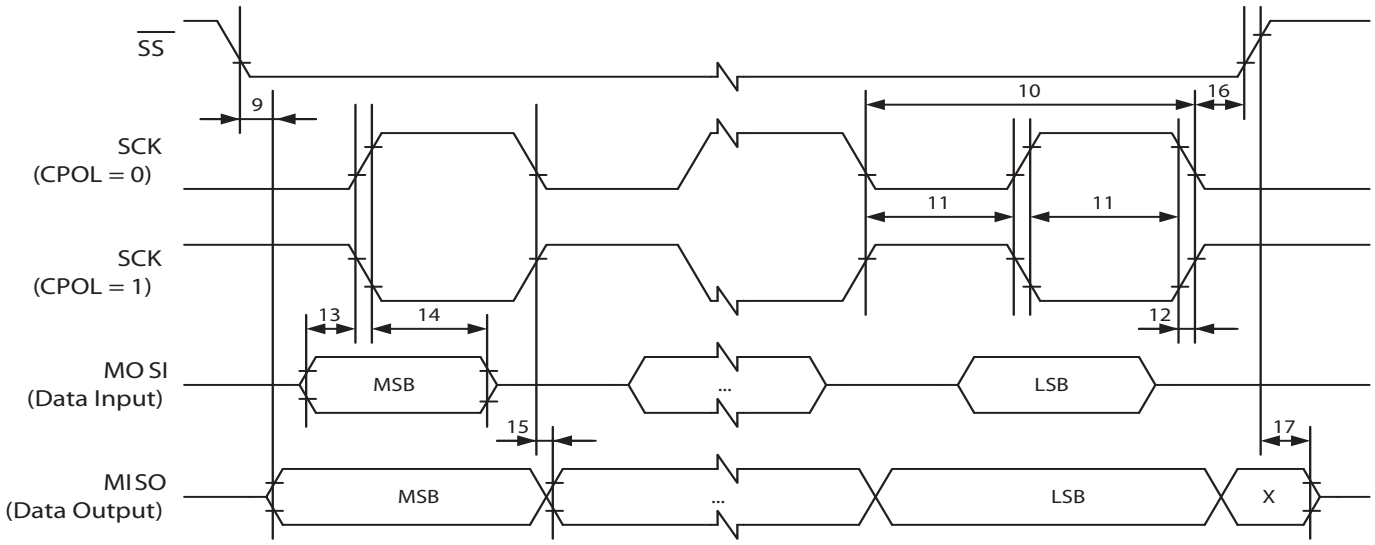
The table below describes the requirements for devices connected to the SPI. The ATVaultIC460 SPI meets or exceeds these requirements under the noted conditions.

See Figure 3-2 for details.

Table 3-5. SPI Timing Parameters

See figure	Description	Condition	Min	Typ	Max	Unit
9	$\overline{SS}$ low to out			TBD		ns
10	SCK period			TBD		ns
11	SCK high/low			TBD		ns
12	Rise/Fall time			TBD		ns
13	Setup			TBD		ns
14	Hold			TBD		ns
15	SCK to out			TBD		ns
16	SCK to $\overline{SS}$ high			TBD		ns
17	$\overline{SS}$ high to tri-state			TBD		ns
18	$\overline{SS}$ low to SCK			TBD		ns

Figure 3-2. SPI Timings



3.5 Connexions for Typical Application

Figure 3-3. ATVaultIC460 connexions for **USB** typical application

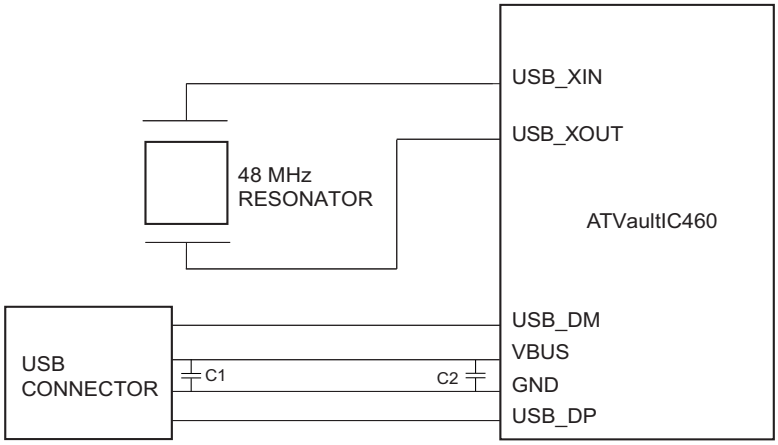


Figure 3-4. ATVaultIC460 connexions for **I²C** typical application

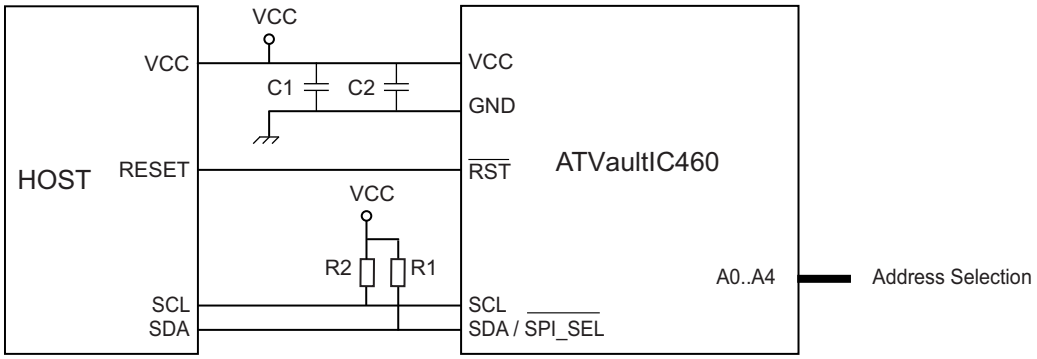


Figure 3-5. ATVaultIC460 connexions for **SPI** typical application

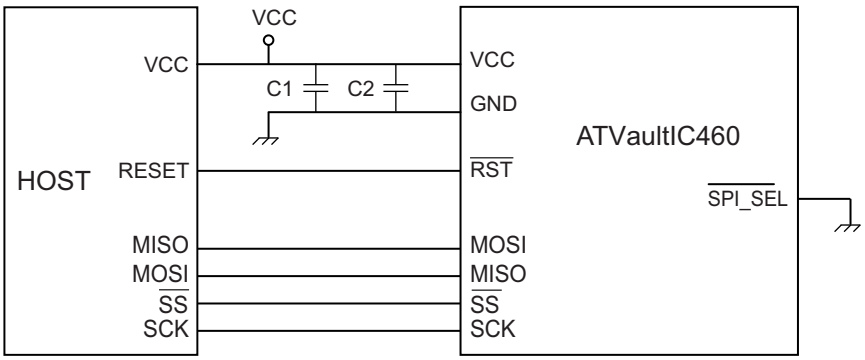


Figure 3-6. ATVaultIC460 connexions for **ISO7816** typical application

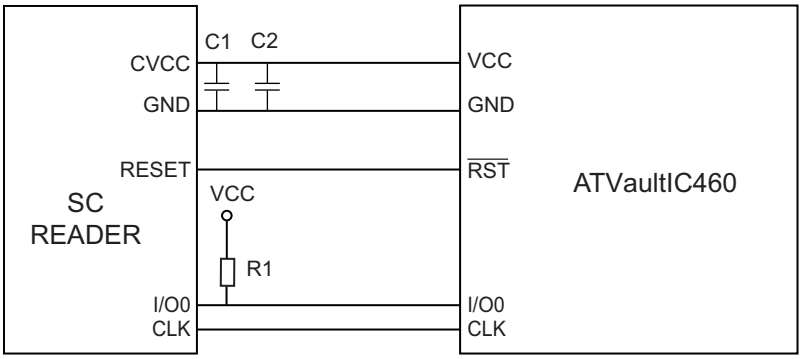


Table 3-6. External components, Bill of Materials

Configuration	Reference	Description	Typ.Value	Comment
USB		Ceramic Oscillator	48MHz	
	C1	Power Supply Decoupling Capacitors	4.7 µF	Recommended
	C2	Power Supply Decoupling Capacitors	10 nF	Recommended
I^2C	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

3.5.1 Internal Oscillator characteristics

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

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	%

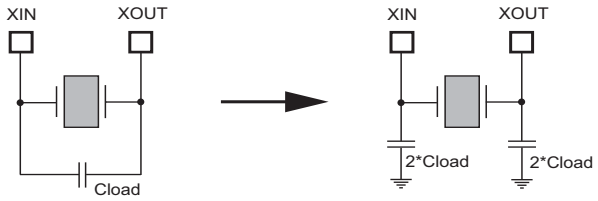
Code	Parameter	Condition	Min.	Typ.	Max.	Unit
Ton	Startup time				1	ms
Pon	Drive level				500	µW
ESR	Equivalent Serie Resistance	@ 48Mhz			70	Ω
Cm	Motional capacitance	@ 48MHz	10		200	fF
Cshunt	Shunt capacitance				6.2	pF
Cload	Load capacitance	Max external capacitors: 12pF	2		6	pF
Idd stdby	Standby current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

The resonator must be placed as close as possible to the ATVaultIC460 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



Atmel recommends to use the ceramic resonator CERALOCK® from *Murata* with the part number *CSTCW48M0X11Mxx-R0* (thin resonator for Smart Card) or *CSTCZ48M0X11Rxx-R0* (small resonator for any system). This ceramic resonator hosts built-in capacitance in a small monolithic chip type. Its electrical properties best fit the Atmel specifications.

3.5.2 Building a USB Token

A **USB reference design** is available for the ATVaultIC460 chip. Atmel offers a complete software and hardware solution based on a full USB communication stack, an ICCD compliant library and a USB dongle as target. The TPR0278 application note *USB ICCD Implementation* describes how to build a USB-ICC and how to implement an application based on the USB ICCD class.

Figure 3-8. USB Token schematic - Reference design

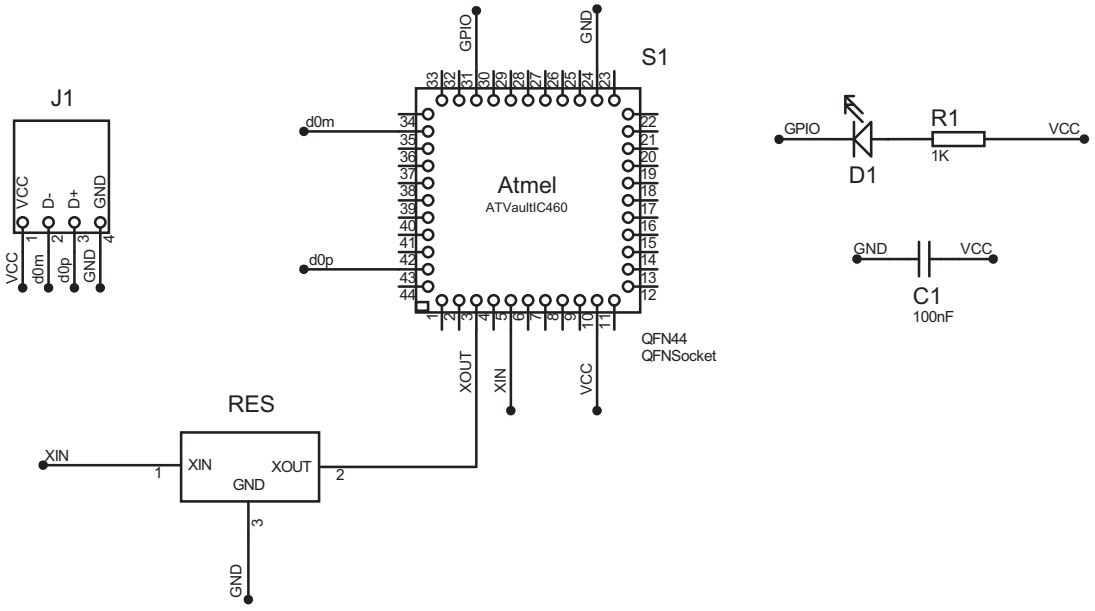


Table 3-8. Bill Of Material - Reference design

Name	Designation	Constructor Ref
S1	Microcontrollor in QFN44 package	Atmel ATVaultIC460
RES	48 Mhz ceramic resonator	Murata CSTCW48M0X11xx
J1	Plug USB Type A	Molex 48037-2000
C1	100 nF capacitance	-
R1	1K resistor	-
D1	Diode LED	KP-3216MGC

3.6 Pin & Package Configuration

3.6.1 Pin Configuration

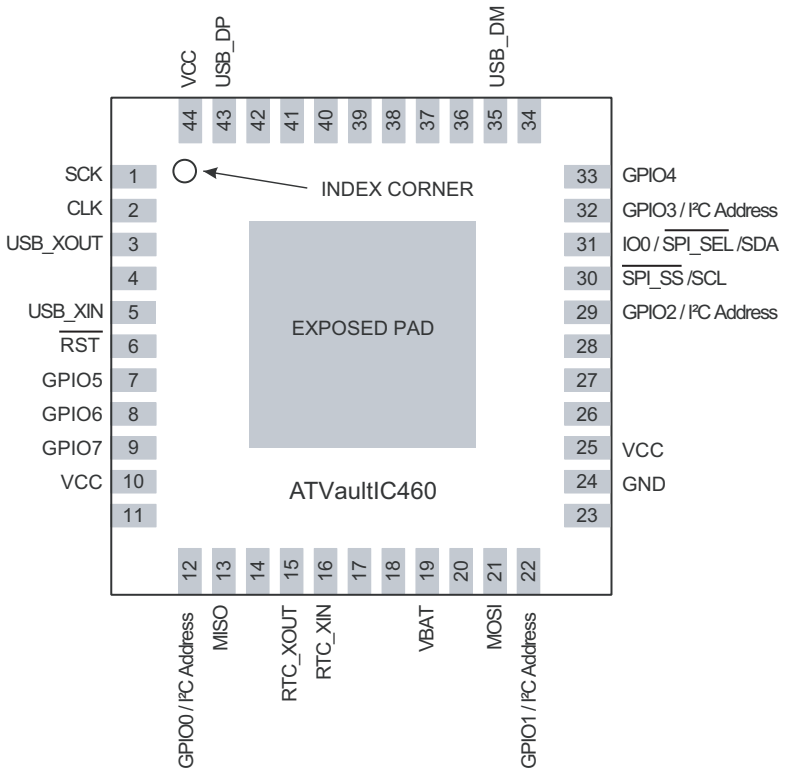
Table 3-9. Pin List Configuration

Designation	Pin #				Description
	QFN 44	SOIC8/USB	SOIC8/SPI	SOIC8/ISO	
SPI_SCK	1	-	5	-	SPI clock
ISO_CLK	2	-	-	5	ISO7816 Clock
USB_XOUT	3	6	-	-	Resonator Signal Input
USB_XIN	5	7	-	-	Resonator Signal Output
$\overline{\text{RST}}$	6	-	6	7	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	8	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	1	Ground (reference voltage)
GPIO2	29	-	-	-	General Purpose IO 2 / I²C Address
$\overline{\text{SS}}$ / SCL	30	2	3	2	SPI Slave Select or I²C SC
$\overline{\text{SPI\_SEL}}$ / SDA / IO0	31	3	4	3	SPI/I²C selection PIN or I²C SDA or ISO7816 IO0
GPIO3	32	-	-	-	General Purpose IO 3 / I²C Address
GPIO4	33	-	-	4	General Purpose IO 4
USB_DM	35	4	-	-	USB D- differential data
USB_DP	43	5	-	-	USB D+ differential data

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

3.6.2 Pinouts for packages QFN44 and SOIC8

Figure 3-9. Pinout ATVaultIC460 - 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 ATVaultIC460 - Package SOIC8 - USB configuration

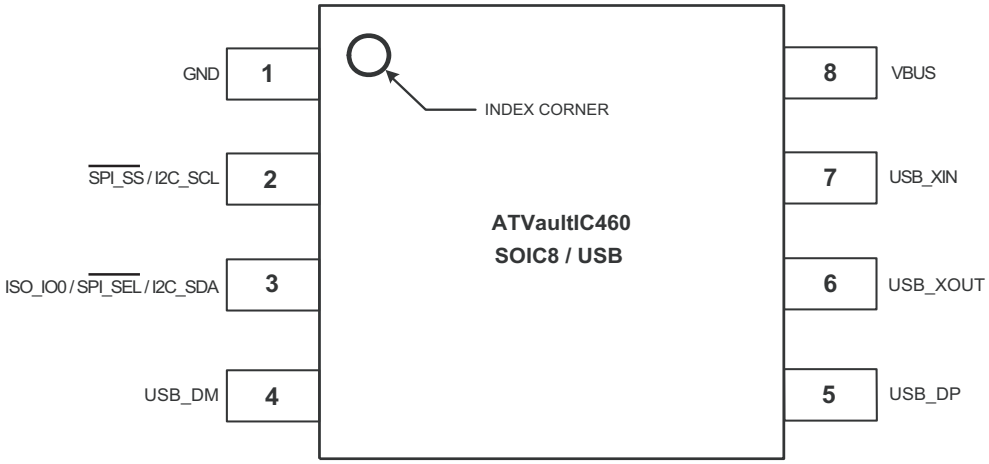


Figure 3-11. Pinout ATVaultIC460 - Package SOIC8 - SPI and I²C configurations

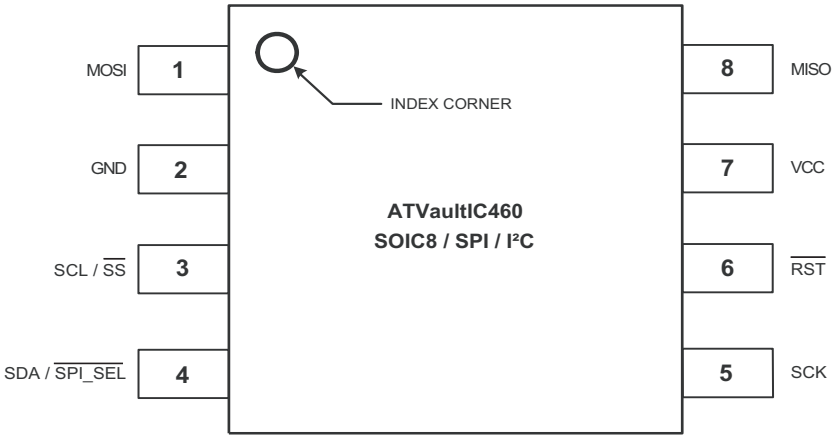
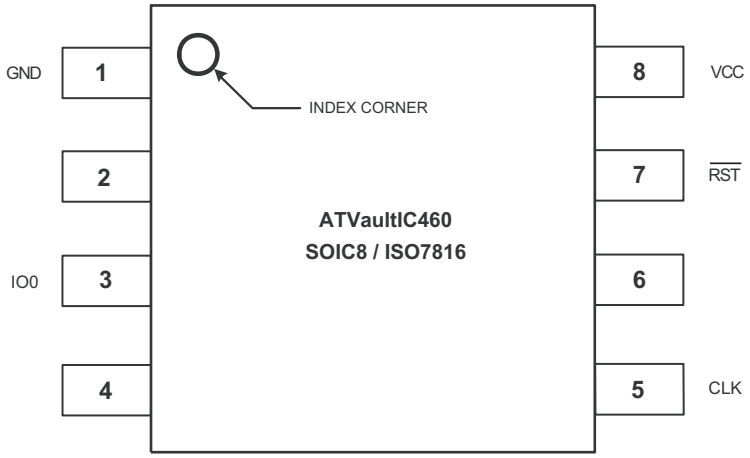
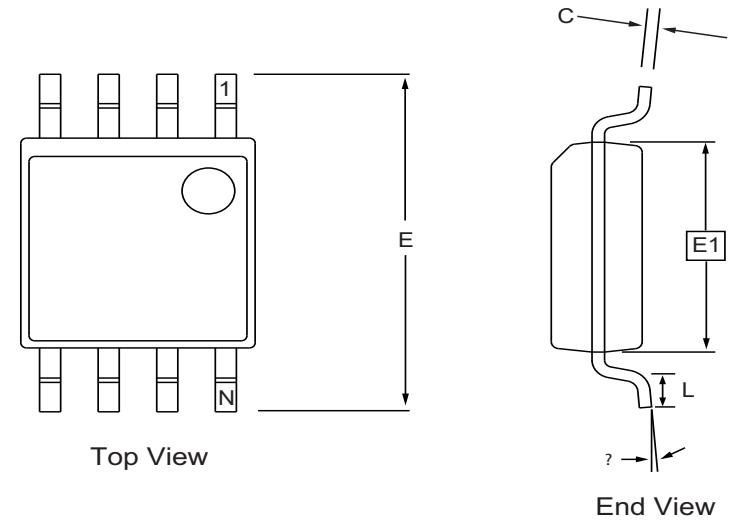


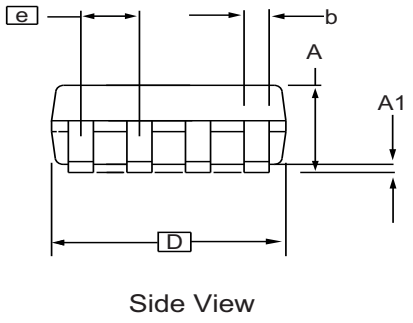
Figure 3-12. Pinout ATVaultIC460 - Package SOIC8 - ISO configuration



3.6.3 Packages characteristics

Figure 3-13. SOIC-8 package characteristics



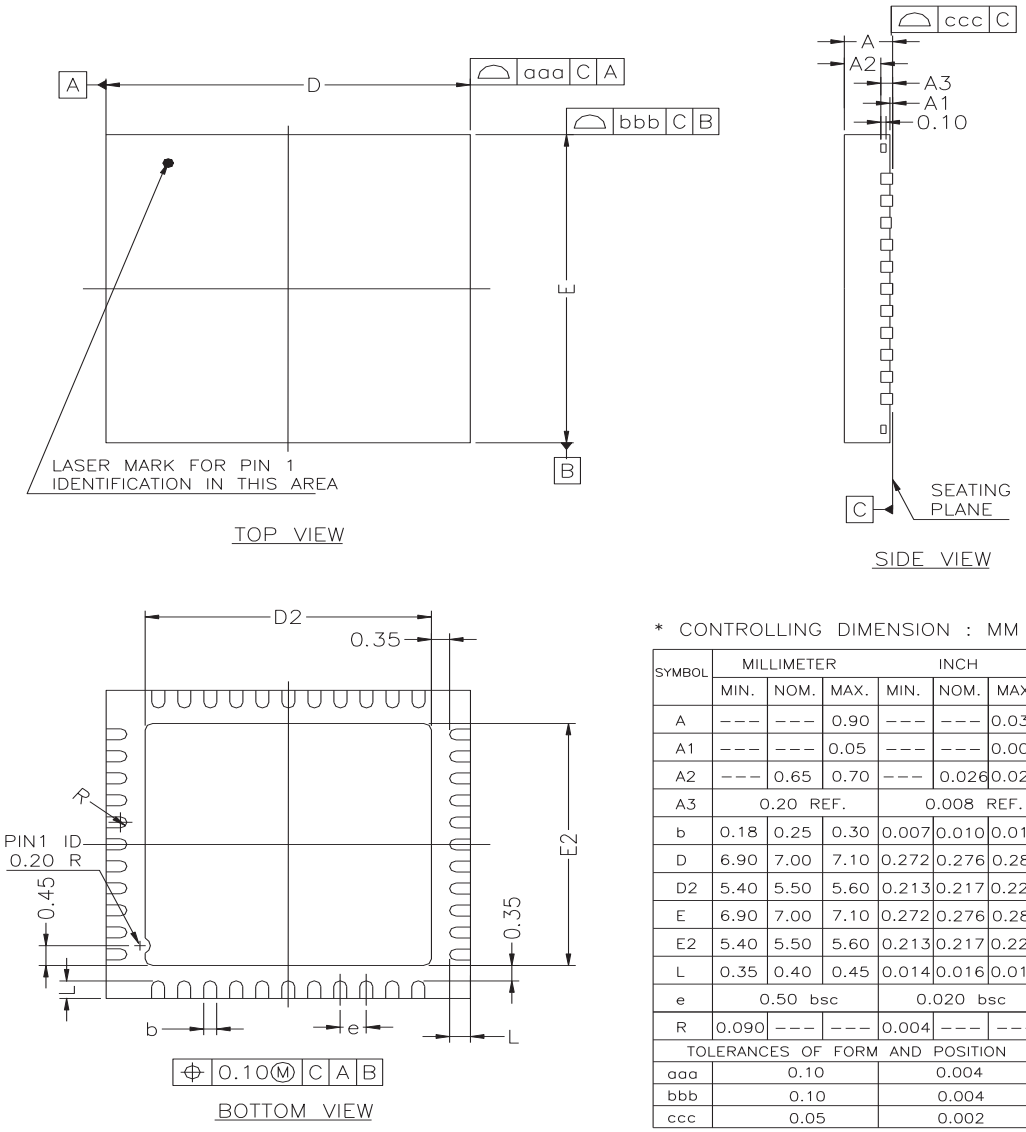


COMMON DIMENSIONS
(Unit of Measure = mm)

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 3-14. 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.

Definitions and abbreviations

3DES / TDES	Triple DES algorithm
AES	Advanced Encryption Standard algorithm as defined in FIPS PUB 197
APDU	Application Protocol Data Unit as defined in ISO7816-3
Authentication	An identification or entity authentication technique assures one party (the verifier), through acquisition of corroborative evidence, of both the identity of a second party involved, and that the second (the claimant) was active at the time the evidence was created or acquired. (From Handbook of Applied Cryptography)
ASSP	Application Specific Standard Product
CBC	Cipher Block Chaining method applied to block ciphers
CFB	Cipher Feedback Register chaining method applied to block ciphers
CCID	Circuit(s) Cards Interface Devices
CMAC	Cipher-based Message Authentication Code
CPU	Central Processing Unit
Cryptographic key	A bit string used as a secret parameter by a cryptographic algorithm. To prevent a key from being guessed, keys need to be generated truly randomly and contain sufficient entropy.
DES	Data Encryption Standard algorithm as defined in FIPS PUB 46-3
Device	Any CPU with master or slave capability
DSA	Digital Signature Algorithm as defined in FIPS PUB 186-2
ECB	Electronic Code Book chaining method applied to block ciphers
ECDSA	Elliptic Curves DSA as defined in FIPS PUB 186-2
EEPROM	Electrically Erasable Programmable Read-Only Memory
FAT	File Allocation Table - file system from Microsoft®
FIPS	Federal Information Processing Standards
FIPS-approved	An algorithm or technique that is specified or adopted in FIPS
HMAC	Hash-based Message Authentication Code as defined in FIPS PUB 198
Host	Entity that communicates (directly or not) with the device.
HOTP	HMAC-based One Time Password algorithm as defined in RFC 4226
ISO7816	Smart Card interface
MAC	Message Authentication Code - A bit string of fixed length, computed by a MAC generation algorithm, that is used to establish the authenticity and, hence, the integrity of a message.
Master	The device that initiates and terminates a transmission. The Master also generates the clock for synchronous interface.
NIST	National Institute of Standards and Technology
NVM	Non Volatile Memory (EEPROM, flash, …)

OFB	Output Feedback Register chaining method applied to block ciphers
PC/SC	Workgroup defining a standard architecture for integration of smart cards in computers
RSA	Rivest Shamir Adleman algorithm
SCP	Secure Channel Protocol as defined by GlobalPlatform
SHA	Secure Hash Algorithm
Slave	The device addressed by a master
SPI	Serial Protocol Interface
Strong Authentication	Exchange of messages during which a claimant proves its identity to a verifier by demonstrating its knowledge of a secret but without revealing it
TWI / I^2C	Two Wire Interface and Inter Integrated Circuit Bus respectively
USB	Universal Serial Bus as defined in USB 2.0 standard

Referenced Documents

[1] ATMEL Corporation. AT98SO Generic Datasheet. TPR0395AX-July2009 (Availbale under Non-Disclosure Agreement signed with ATMEL).

[2] NIST SP 800-63 - Electronic Authentication Guideline - April 2006

[3] ISO9798 - 2 Entity Authentication - Part 2 : Mechanisms using symmetric encipherment algorithms. July 1999

[4] FIPS PUB 196. Entity Authenticationusing public key cryptography. Feb 1997.

[5] RSA Laboratories. PKCS #11 v2.20: Cyrptograhic Token Interface Standard. June 2004.

[6] Microsoft - Smart Card Minidriver Specification for Windows Base Cryptographic Service Provider (Base CSP) and Smart Card Key Storage Provider (KSP) version 5.07 - September 2007

[7] Atmel Corporation. How to secure Video Slot Gaming Machines using VaultIC™ Security Modules? TPR443AX-September 2009

[8] Universal Serial Bus Specification Revision 2.0. April 2000.

Datasheet Revision History

Rev AX - 15 July 2009 : Initial Version

Rev BX - 29 September 2009 : Update Product Name

1 Overview 3

1.1 Tampering resistance 3

1.2 Authentication capability 3

1.3 Secure storage 4

1.4 Flexibility 4

1.5 Typical application 5

1.6 Ordering Information 5

1.6.1 Legal 5

1.6.2 Quotation and Volume 5

1.6.3 Part Number 6

1.6.4 Starter Kit 6

1.6.5 Demo Kit 6

1.7 Software and Hardware Architecture 7

2 Detailed Features 8

2.1 Communication Interfaces 8

2.2 Security Mechanisms 8

3 Product Characteristics 10

3.1 Command Timings (T=25°C) 10

3.2 Maximum Ratings 11

3.3 AC/DC Characteristics (2.7V - 5.5V range; T= -25°C to +85°C) 11

3.4 Timings 13

3.4.1 I²C Timings 13

3.4.2 SPI Timings 14

3.5 Connexions for Typical Application 15

3.5.1 Internal Oscillator characteristics 16

3.5.2 Building a USB Token 17

3.6 Pin & Package Configuration 19

3.6.1 Pin Configuration 19

3.6.2 Pinouts for packages QFN44 and SOIC8 20

3.6.3 Packages characteristics 22

Headquarters

Atmel Corporation
2325 Orchard Parkway
San Jose, CA 95131
USA
Tel: 1(408) 441-0311
Fax: 1(408) 487-2600

International

Atmel Asia
Unit 01-05 & 16, 19/F
BEA Tower, Millennium City 5
418 Kwun Tong Road
Kwun Tong, Kowloon
Hong Kong
Tel: (852) 2245-6100
Fax: (852) 2722-1369

Atmel Europe
Le Krebs
8, Rue Jean-Pierre Timbaud
BP 309
78054 Saint-Quentin-en-
Yvelines Cedex
France
Tel: (33) 1-30-60-70-00
Fax: (33) 1-30-60-71-11

Atmel Japan
9F, Tonetsu Shinkawa Bldg.
1-24-8 Shinkawa
Chuo-ku, Tokyo 104-0033
Japan
Tel: (81) 3-3523-3551
Fax: (81) 3-3523-7581

Product Contact

Web Site
www.atmel.com

Technical Support
at98sc@atmel.com

Sales Contact
www.atmel.com/contacts

Literature Requests
www.atmel.com/literature

TPR0441BX–SMS–09/09