



## HEADQUARTERS

### ATMEL CORPORATION

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

## INTERNATIONAL

### Atmel Asia Limited

Unit 01-5 & 16, 19/F Bea Tower  
Millenium 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

# Crypto Products

# Customer Guide

2nd QUARTER 2009

Disclaimer: The information in this document is provided in connection with Atmel products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Atmel products. EXCEPT AS SET FORTH IN ATMEL'S TERMS AND CONDITIONS OF SALE LOCATED ON ATMEL'S WEB SITE, ATMEL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ATMEL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ATMEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Atmel makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Atmel does not make any commitment to update the information contained herein. Unless specifically provided otherwise, Atmel products are not suitable for, and shall not be used in, automotive applications. Atmel's products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.

© 2009 Atmel Corporation. All rights reserved. Atmel®, Atmel logo and combinations thereof, AVR®, CryptoMemory®, CryptoRF® and others are registered trademarks, CryptoCompanion™, CryptoController™, CryptoAuthentication™ and others are trademarks of Atmel Corporation and its subsidiaries. Other terms and product names may be trademarks of others.



## Table of Contents

### Table of Contents

<b>What's New with Crypto Products .....</b>	<b>3</b>
<b>Application Highlights .....</b>	<b>5</b>
<b>Crypto Products Overview .....</b>	<b>7</b>
<b>Product Selection Guide .....</b>	<b>13</b>
<b>Packaging Information .....</b>	<b>16</b>
<b>Documentation .....</b>	<b>18</b>
<b>Ordering Information .....</b>	<b>22</b>
<b>Contacts .....</b>	<b>Error! Bookmark not defined.</b>

# What's New with Crypto Products

---

## CryptoAuthentication™

CryptoAuthentication™ is a new family of low cost, one-wire, ultra low power, super secure cryptographic authentication ICs with an embedded SHA-256 engine and a 256-bit cryptographic key. The chips incorporate Atmel's latest security design features and securely authenticate any item to which it is attached.

The most common use of the CryptoAuthentication chip is to prevent software in an embedded system from being cloned or to validate downloaded software updates. But, the 3-pin SOT23 package also makes it an ideal solution for the authentication of replaceable or consumable components in handheld electronics and/or compact medical devices. CryptoAuthentication provides system developers an unprecedented combination of security and ease of use at a cost lower than the competition.

### Application Examples

- Software anti-piracy in any embedded system
- Key exchange for encrypted downloads
- Authentication of replaceable items
- Network or computer access control
- Portable media players & GPS systems
- Prevention of clones for demonstration and evaluation boards
- Anti-clone authentication for daughter cards
- Physical access control

### Key Features

- Secure authentication & key exchange
- Superior SHA-256 Hash Algorithm
- Best in class 256 bit key length
- Guaranteed Unique 48 bit Serial Number
- High speed single wire interface
- <100nA Sleep Current
- Multi-level hardware security
- Secure personalization

## Rhino+ Evaluation Kit

The Rhino+ kit is low cost demonstration and evaluation kit for the AT88SA102S CryptoAuthentication IC. The kit is AVR® based includes libraries and comprehensive documentation. Developers will find easy demonstrations software and with a very convenient USB interface that allows users to experiment with CryptoAuthentication on a PC. The board includes an alternate 3 pin connection that allows for full system development when connected to an Atmel STK600. Atmel has available embedded source code fully operational on AVR and ARM.

## PowerPoint Training Slide Available on Sales Portal

Updated combat tools are available on Atmel's Sales Portal, including a new Crypto Products Portfolio Training Presentation that is designed to help you present the most up-to-date information.

Click below to go to the sales portal:

<http://intra.cso.atmel.com/marcom/CSO%20product%20information/CryptoMemory/sales.html>

## CryptoRF Epoxy Glass Tag Flyer

Crypto Products have developed a new CryptoRF Epoxy Glass Tag flyer to assist with describing the various transponder tags options currently supported in the CryptoRF product offering. This flyer is available on the websites as a downloadable PDF file.

## Documentation

### New Datasheets

- New: AT88SA102S – CryptoAuthentication 03/09
- New: AT88SA10HS – CryptoAuthentication Host 06/09
- New: AT88SA100S – CryptoAuthentication Battery 06/2009
- New: AT88SCXXXXCA – CryptoMemory® Low Density Full Spec 05/09



### ***New Application Notes***

- New: Using 2.7V – 3.6V CryptoMemory® Devices in 5V Designs 02/09
- New: Using CryptoMemory® in Full 12C Compliant Mode 03/09
- New: QFN Package Mounting Guidelines for AT88RF1354 – 04/09
- New: CryptoAuthentication™ AT88SA102S Hardware Reference Design 05/09
- New: CryptoAuthentication™ Product Uses for AT88SA102S and AT88SA10HS 03/09
- New: CryptoAuthentication™ High Level Security Modes 03/09

### ***New White Paper***

- New: 256 Bit Key – Is It Big Enough? 03/09

### ***New Flyers***

- New: CryptoRF Epoxy Glass Tags Flyer

# Application Highlights

---

## Embedded Software Clone Prevention – CryptoAuthentication

Companies can find that overnight their embedded software or intellectual property (IP) appears in the product of a competitor. The counterfeiter carries virtually no R&D cost, and can therefore undercut the legitimate supplier on price and steal market share. Companies looking for an inexpensive way to protect their embedded software from competitors and counterfeiters can now use the AT88SA102S for onboard hardware authentication.

CryptoAuthentication's AT88SA102S can easily be integrated into any application for anti-cloning protection of embedded software. At random intervals a challenge is sent to the CryptoAuthentication device. The response from the CryptoAuthentication is then compared to the expected response. By providing a large number of challenges implemented in clever ways and placing those in unique areas, the source code can be relatively well protected. This makes it extremely difficult for anyone to reverse engineer the source code.

## Battery Authentication – CryptoAuthentication

The continuing growth of portable handheld devices has created an ever growing problem of counterfeit battery packs. Both the OEM and end users pay a price when counterfeit battery replacements are chosen. The impact of imitation battery packs to the original equipment manufacturer includes increased safety risks for their customers, greater product returns, reduced customer satisfaction, and a reduction in revenue for batteries supplied by the OEM.

The AT88SA100S CryptoAuthentication device provides an integrated solution that will stop counterfeiters. The AT88SA100S chip is added to the battery pack circuitry. The chip is used in conjunction with the handheld device microprocessor to verify the AT88SA100S before the device will accept the battery as authentic. Manufacturers can stop the use of counterfeit batteries altogether or they can choose to allow diminished performance. CryptoAuthentication can also be implemented to allow manufacturers to track when a user attempts to use unauthorized batteries so that false warranty claims can be avoided. Atmel also carries a line of battery management ICs that include an authentication function. CryptoAuthentication is a solution for battery packs that do not require an AVR smart battery IC but where very low cost authentication is required.

## Sub-System Board Authentication – CryptoMemory

Many systems in the field today are supported via ongoing maintenance or repair programs. Periodically, sub-system PCB's (i.e. boards for PCs, gaming machines, vending machines, test equipment, peripherals, blade servers, etc ...) are replaced during the useful lifetime of the product. How does the OEM insure one of their boards is installed when replacement is required, and not a lower quality clone? Adding CryptoMemory to the board enables a secure authentication scheme between the replaced board and the main controller board, insuring an authentic OEM unit is installed. Additionally, CryptoMemory can securely store usage data if desired. Why is this important? Clearly, it preserves the OEM's revenue stream from spare parts replacement, and insures high-quality replacement boards are installed, reducing ongoing maintenance support costs.

## Secure data logging of high value modules – CryptoRF

Servicing high value modules can often present logistical problems to repair centers and personnel. The service could be for standard maintenance work or for warranty claims. The high value nature of the item to be serviced is sometimes accompanied with difficult physical access to the item in question. In cases such as this, CryptoRF and our Reader IC provide an option for improving the service process. Using our efficient reference design for the Reader IC, users can integrate a CryptoRF reader into their product with minimal cost and area impact. This integrated reader is dedicated to writing or data logging system event information to a CryptoRF tag. The CryptoRF tags are inserted into the high value modules at the time of manufacture. When a repair technician begins the service process, the data log information is read from the CryptoRF tag with a second reader. This enables the capturing of the system events even while access to the finished module may be impossible – the module may have been electrically destroyed in a harsh environment.

## Protecting Home and Business Networks - CryptoController™

In home networking applications like femtocell boxes, it is important to provide a way to mutually authenticate the femtocell with the remote network. Femtocells are typically used in residential and small business environments where cell phone coverage is poor. The femtocell is simply connected to the service provider's network via DSL or cable allowing existing cell phones to gain coverage where none existed previously. Before allowing access to a network the remote host must securely identify that the femtocell is trusted and authorized. By using CryptoController™ a 2048-bit RSA key pair can be generated while securely storing the private key in tamper proof CryptoController hardware. This key pair facilitates Public Key Infrastructure allowing both nodes to mutually authenticate each other. During platform initialization (manufacturing) a root certificate can also be securely stored in CryptoController's protected NV memory. By using a Public Key Infrastructure (PKIC) facilitated by the CryptoController key pair, the root certificate can be securely transmitted from the femtocell to the remote node in order to show that the platform is genuine and trusted.

# Crypto Products Overview

---

## CryptoAuthentication

CryptoAuthentication is a family of cost effective authentication chips and the first low cost authentication product to implement the SHA-256 hash algorithm, which is part of the latest set of algorithms recommended by the US Government. Each CryptoAuthentication chip contains a pre-programmed serial number that is guaranteed to be unique and additional fuse bits for one-time programming of customer specific information.

The 1 wire interface makes connection to the device simple and reduces the number of GPIO or UART resources required for the host microcontroller. When the crypto operations are complete the device automatically goes into sleep mode reducing the standby current to less than 100nA. The CryptoAuthentication devices are packaged in a very tiny 3-pin SOT 23 which has a foot print of 2mm x 3mm, making it an ideal solution for space constrained portable systems or battery packs.

The CryptoAuthentication family includes the two client chips the AT88SA102S and then AT88SA100S, as well as a supporting host chip the AT88SA10HS. The host device stores the host side keys and implements the entire crypto code in hardware so no security expertise is required by the system designer.

- AT88SA102S – general purpose authentication
- AT88SA100S – battery pack authentication
- AT88SA10HS – host side security IC

CryptoAuthentication incorporates the latest security features developed from a long history of security chip design expertise. The chips have full metal shields over the entire internal circuitry, so that if an attacker cuts or shorts any wire in the shield, the chip stops functioning. Added to this are internal clocks and voltage generation, fully encrypted memories, tamper detection and fully secure production test methods.

## CryptoMemory

CryptoMemory has many features that make it the only product on the market to supply low cost and high security solutions for embedded applications.

With memory densities from 1-Kbit to 256-Kbits, CryptoMemory is able to store and protect small to medium amounts of data while offering four different levels of security: Free access for use as straight memory, password protection using a choice of 8 sets of separate read/write passwords, mutual authentication using a choice of 4 sets of 64-bit keys, and full data encryption for complete confidentiality. These 4 levels of security, 8 unique passwords and 4 unique keys may be applied independently to the multiple sectors that the memory is divided into.

## CryptoRF

CryptoRF uses exactly the same cryptographic algorithms as CryptoMemory providing customers the same features and security. CryptoRF is a 13.56 MHz RFID device family with a 64-bit embedded hardware encryption engine, dual authentication capability, and up to 64-Kbits of user memory. Based on the royalty-free ISO 14443-B standard, CryptoRF is ideally suited to meet a variety of security applications such as contactless payment, product authentication, patient safety, and patron management.

CryptoRF devices are great for proximity applications where hardware security is desired or when environmental factors such as dirt, moisture, chemicals, etc., exist.

CryptoRF devices are available with EEPROM densities from 1-Kbit to 64-Kbits of user memory to accommodate a wide range of information storage and cost requirements. The user memory itself may be divided into as many as 16 separate sections, each of which can be customized to allow different levels of read and write access, including:

- Free access EEPROM
- Password protection
- Authentication
- Data encryption and message authentication codes (MAC's)

These user selectable optional security features give customers tremendous flexibility in developing and deploying a secure RF solution. CryptoRF is deliverable as modules for creation of complete RFID tags, RFID cards and thinned wafers.

## CryptoRF Reader

Our new reader IC, AT88RF1354, performs all RF communication, packet formatting, decoding, and communication error checking and is based on the ISO/IEC 14443-2 Type B signal modulation scheme and ISO/IEC 14443-3 Type B frame format, used by more than 60% of the vendors of RFID host readers. Data is exchanged half duplex at a 106k bit per second rate. A two-byte CRC\_B provides communication error detection capability. The AT88RF1354 can be used with both RFID transponders and contactless smart cards and is compatible with 3.3V and 5V host microcontrollers with two-wire or SPI serial interfaces.

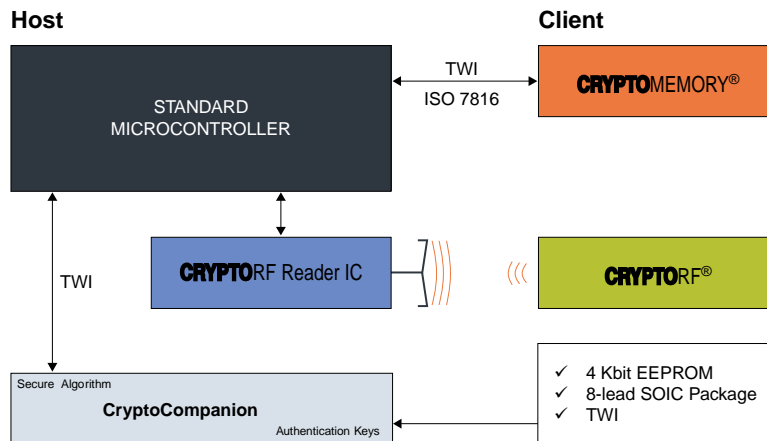
The highly integrated reader IC requires fewer external components than competing RFID reader chips, resulting in a lower BOM. The reader chip comes in the **smallest footprint** available today for 13.56 MHz reader chips and is packaged in a 6mm x 6mm, 36-pin QFN.

## CryptoCompanion™ – For Host Side Security

This companion chip, the AT88SC018, implements the algorithms and the entire protocol completely in hardware. It is fully tested and guaranteed to work properly with all CryptoMemory/CryptoRF chips. The system designer doesn't have to design the software and also doesn't have to test it.

To validate the authenticity of a consumable or replaceable item (client) connected to a system (host), there must be some secret information stored in both the client and the host. CryptoMemory and CryptoRF provide the ideal solution for the client side and CryptoCompanion™ secures the host side.

CryptoCompanion can play a key role for customers whose future revenue stream depends on the continued sale of consumable, replaceable, or add-in components such as batteries or test strips in a portable medical analyzer.



## CryptoController

CryptoController, Atmel's embedded Trusted Platform Module (TPM) is a complete turnkey solution providing ultra-strong security for both PC and embedded systems. Primary TPM capabilities include IP protection, system integrity, authentication, and secure communication. The core building blocks in CryptoController are our AVR microcontroller and our expertise in silicon security technologies. Additional security measures include a variety of tamper-evident circuits such as voltage, temperature and frequency tampers. Available in 28-TSSOP and space saving 40-lead QFN (MLF) packages, CryptoController provides a cost effective solution for all computing devices.

### ***Features include:***

- Full Trusted Computing Group (TCG) v1.2 rev. 103 specification compliance
- 2048-bit RSA hardware crypto accelerator
- Hardware SHA-1 accelerator, 50us/64-byte block
- On-chip storage of up to 21 2048-bit RSA key pairs
- Reliable true hardware random number generator
- 3.3v operation
- Multiple I/O options: LPC, TWI, and SPI

## CryptoMemory Kits

Name	Function	Ordering Code	Detailed Description	Kit Contents	Avail
Aris	Easily add CryptoMemory security to the customer's existing system; can be used with Atmel AVR and ARM starter kits.	AT88SC-DK1	Adapts CryptoMemory to existing development environments with a 2-Wire interface. Comes complete with Crypto Core Development Library and evaluation/demonstration support on ATSTK500.	Aris Adaptor board, cables, CD, CryptoMemory samples, Quick Start Guide.	Now
Aris+*	Includes CryptoMemory security in new applications Microcontroller and development board included, requires PC.	AT88SC-ADK2	Low-cost development kit for CryptoMemory and CryptoCompanion chips on an AVR platform. Features menu-driven Crypto Evaluation Studio and Crypto Core Development Library. Library architecture permits code porting to other microcontrollers.	Aris+ board, CD, USB cable, Quick Start Guide, CryptoMemory SOIC samples, CryptoCompanion SOIC samples.	Now



\*Flagship Kit

## CryptoRF Kits (RFID)

Name	Function	Ordering Code	Detailed Description	Kit Contents	Avail
Keen+*	Lowest cost reader reference design; uses Atmel reader IC on an AVR platform.	AT88SCRF-ADK2	An all Atmel development kit using CryptoRF based on an AVR platform. Well-documented Crypto Core development library. Library architecture permits code porting to other microcontroller platforms. Connectivity to PC and power via USB.	Keen+ combo module and evaluation board, CD, USB cable, Quick Start Guide, CryptoRF tag and card assortment.	Now
Yuma+	Great for secure RFID developers who prefer an AVR platform.	AT88SCRF-ADK1	Complete development kit for secure RFID applications using CryptoRF. Combines Melexis MLX90121 reader IC and Atmel AVR microcontroller technologies to feature a firmware enabled RF reader module reference design that exposes a simple SPI API. Fully supported by the menu-driven Crypto Evaluation Studio from Atmel.	Yuma+ module and module evaluation boards, CD, USB cable, Quick Start Guide, CryptoRF tag and card assortment.	Now
CryptoRF/SkyeTek	For secure RFID developers who prefer an ARM platform with a SkyeTek reader.	AT88SCRF-S7DKP	Secure RFID demonstration kit featuring Atmel's CryptoRF secure tag and SkyeTek's M2 derivative reader technologies on an ARM platform. Includes SkyeTek's SkyeWare evaluation/demonstration software and an option to license MetaFi™ development API from SkyeTek.	CryptoRF/SkyeTek module and evaluation boards, Embedded CD, USB cable, Quick Start Guide, CryptoRF cards.	Now

\*Flagship kit

## CryptoController (TPM) Kits

Name	Function	Ordering Code	Detailed Description	Kit Contents	Avail
CryptoController TWI	Embedded TPM development kit based on AVR.	AT97SC3204T-X1A180	Embedded TPM development kit based on the AVR AT90USBKey kit with an added Embedded TPM TWI Module and Embedded TPM demonstration, development, and evaluation software.	Embedded TPM Module board, containing a 1.2 TWI Trusted Platform Module; AT90USBKey board; Standard A to mini B USB device cable; Mini A to receptacle A USB host adapter; 9-Volt battery alternate supply cable; USB Flash Drive, containing documentation and demonstration software.	July 2009

## CryptoAuthentication Kits

Name	Function	Ordering Code	Detailed Description	Kit Contents
Rhino+	Very low cost and easy demonstration and evaluation in PC environment	AT88SA-ADK1	AVR based demonstration and evaluation kit for CryptoAuthentication (AT88SA102S). Just plug into your USB port and download the demo application.	Rhino+ board, Quick Start Guide

# Product Selection Guide

## CryptoAuthentication

Part No.**	Org	Voltage	Description	I/O*	RoHS	Temp	Avail
AT88SA102S	N/A	2.5-5.5V	SHA-256 authentication with high speed single wire interface and less than 100nA sleep current.	1	Yes	-40°C to 85°C	DV Samples Now Production October 09
AT88SA10HS	N/A	2.5-5.5V	Host side security IC for CryptoAuthentication AT88SA102S and AT88SA100S.	1	Yes	-40°C to 85°C	DV Samples Now Production October 09
AT88SA100S	N/A	2.5-5.5V	SHA-256 battery authentication with high speed single wire interface and less than 100nA sleep current.	1	Yes	-40°C to 85°C	DV Samples Now Production October 09

**Note:** \*CryptoAuthentication DVS part numbers for quotes and opportunities in Model N are AT88SA102S-DTSU-T, AT88SA10HS-DTSU-T, and AT88SA100S-DTSU-T.

## CryptoMemory with Authentication and Encryption

Part No.**	Org	Voltage	Description	I/O*	RoHS	Temp	Avail
AT88SC0104CA	4x256	2.7 – 3.6	1-Kbit user memory with authentication and encryption, ISO 7816-3 asynchronous and synchronous I2C-Compatible protocols	T=0 TWI	Yes	-40°C to 85°C	Now
AT88SC0104C	4x256	2.7 – 5.5	1-Kbit user memory with authentication and encryption, ISO 7816-3 asynchronous and synchronous 2-wire protocols	T=0 TWI	Yes	-40°C to 85°C	<i>Not recommended for new 3 volt designs</i>
AT88SC0204CA	4x512	2.7 – 3.6	2-Kbit user memory with authentication and encryption, ISO 7816-3 asynchronous and synchronous I2C-Compatible protocols	T=0 TWI	Yes	-40°C to 85°C	Now
AT88SC0204C	4x512	2.7 – 5.5	2-Kbit user memory with authentication and encryption, ISO 7816-3 asynchronous and synchronous 2-wire protocols	T=0 TWI	Yes	-40°C to 85°C	<i>Not recommended for new 3 volt designs</i>
AT88SC0404CA	4x1024	2.7 – 3.6	4-Kbit user memory with authentication and encryption, ISO 7816-3 asynchronous and synchronous I2C-Compatible protocols	T=0 TWI	Yes	-40°C to 85°C	Now
AT88SC0404C	4x1024	2.7 – 5.5	4-Kbit user memory with authentication and encryption, ISO 7816-3 asynchronous and synchronous 2-wire protocols	T=0 TWI	Yes	-40°C to 85°C	<i>Not recommended for new 3 volt designs</i>
AT88SC0808CA	8x1024	2.7 – 3.6	8-Kbit user memory with authentication and encryption, ISO 7816-3 asynchronous and synchronous I2C-Compatible protocols	T=0 TWI	Yes	-40°C to 85°C	Now
AT88SC0808C	8x1024	2.7 – 5.5	8-Kbit user memory with authentication and encryption, ISO 7816-3 asynchronous and synchronous 2-wire protocols	T=0 TWI	Yes	-40°C to 85°C	<i>Not recommended for new 3 volt designs</i>

## CryptoMemory with Authentication and Encryption continued...

Part No.**	Org	Voltage	Description	I/O*	RoHS	Temp	Avail
AT88SC1616C	16x1024	2.7 – 5.5	16-Kbit user memory with authentication and encryption, ISO 7816-3 asynchronous and synchronous 2-wire protocols	T=0 TWI	Yes	-40°C to 85°C	Now
AT88SC3216C	16x2048	2.7 – 5.5	32-Kbit user memory with authentication and encryption, ISO 7816-3 asynchronous and synchronous 2-wire protocols	T=0 TWI	Yes	-40°C to 85°C	Now
AT88SC6416C	16x4096	2.7 – 5.5	64-Kbit user memory with authentication and encryption, ISO 7816-3 asynchronous and synchronous 2-wire protocols	T=0 TWI	Yes	-40°C to 85°C	Now
AT88SC12816C	16x8192	2.7 – 5.5	128-Kbit user memory with authentication and encryption, ISO 7816-3 asynchronous and synchronous 2-wire protocols	T=0 TWI	Yes	-40°C to 85°C	Now
AT88SC25616C	16x16384	2.7 – 5.5	256-Kbit user memory with authentication and encryption, ISO 7816-3 asynchronous and synchronous 2-wire protocols	T=0 TWI	Yes	-40°C to 85°C	Now

**Note:** \*Crypto products are compatible with I2C timing but not all of the protocol

\*\* Secure memory products (AT88SC102, AT88SC1003, AT88SC153 and AT88SC1608) are available to satisfy current business but are not recommended for new designs.

## CryptoRF with Authentication and Encryption

Part No.	Org	Voltage	Description	I/O*	RoHS	Temp	Avail
AT88RF04C	4X1024	N/A	Contactless 4-Kbit user memory with authentication and encryption	ISO/IEC 14443 B	Yes	N/A	Now
AT88SC0104CRF	4x256	N/A	Contactless 1-Kbit user memory with authentication and encryption	ISO/IEC 14443 B	Yes	N/A	Now <i>Not recommended for new designs</i>
AT88SC0204CRF	4x512	N/A	Contactless 2-Kbit user memory with authentication and encryption	ISO/IEC 14443 B	Yes	N/A	<i>Not recommended for new designs</i>
AT88SC0404CRF	4x1024	N/A	Contactless 4-Kbit user memory with authentication and encryption	ISO/IEC 14443 B	Yes	N/A	<i>Not recommended for new designs</i>
AT88SC0808CRF	8x1024	N/A	Contactless 8-Kbit user memory with authentication and encryption	ISO/IEC 14443 B	Yes	N/A	Now
AT88SC1616CRF	16x1024	N/A	Contactless 16-Kbit user memory with authentication and encryption	ISO/IEC 14443 B	Yes	N/A	Now
AT88SC3216CRF	16x2048	N/A	Contactless 32-Kbit user memory with authentication and encryption	ISO/IEC 14443 B	Yes	N/A	Now
AT88SC6416CRF	16x4096	N/A	Contactless 64-Kbit user memory with authentication and encryption	ISO/IEC 14443 B	Yes	N/A	Now

## CryptoRF Reader

Part No.	Org	Voltage	Description	I/O*	RoHS	Temp	Avail
AT88RF1354	N/A	3.0- 5.5	13.56 MHz, ISO 14443 type B RFID reader	TWI SPI	Yes	-40°C to 85°C	Now

## CryptoCompanion

Part No.	Org	Voltage	Description	I/O*	RoHS	Temp	Avail
AT88SC018	N/A	2.7-3.6	Host side security IC for CryptoMemory and CryptoRF	TWI	Yes	-0°C to 70°C	Now

## CryptoController (TPM)

Part No.**	Org	Voltage	Description	I/O*	RoHS	Temp	Avail
AT97SC3204	N/A	3-3.6	Fully v1.2 TCG-compliant security processor, Microsoft® Windows Vista™ logo compliant, secure key generation and storage (up to 21 2048-bit RSA keys stored inside TPM at one time), RNG, SHA-1, 2048-bit RSA crypto accelerator	LPC	Yes	-0°C to 70°C	Production Sep 09
AT97C3204T	N/A	3-3.6	Fully v1.2 TCG-compliant security processor, Microsoft® Windows Vista™ logo compliant, secure key generation and storage (up to 21 2048-bit RSA keys stored inside TPM at one time), RNG, SHA-1, 2048-bit RSA crypto accelerator	TWI	Yes	-0°C to 70°C	Production Sep 09

# Packaging Information

## CryptoAuthentication Packaging Information

Part No.	SOT23 3-pin					
AT88SA102S	✓					
AT88SA10HS	✓					
AT88SA100S	✓					

## CryptoMemory Packaging Information

Part No.	PDIP, 8-lead	SOIC, 8-lead	TSSOP, 8-lead	UDFN** 8-contact	J Module* (preferred)	P Module
AT88SC0104CA	✓	✓	✓	✓	✓	✓
AT88SC0104C	✓	✓				✓
AT88SC0204CA	✓	✓	✓	✓	✓	✓
AT88SC0204C	✓	✓			✓	✓
AT88SC0404CA	✓	✓	✓	✓	✓	✓
AT88SC0404C	✓	✓			✓	✓
AT88SC0808CA	✓	✓	✓	✓	✓	✓
AT88SC0808C	✓	✓			✓	✓
AT88SC1616C	✓	✓			✓	✓
AT88SC3216C	✓	✓			✓	
AT88SC6416C	✓	✓			✓	
AT88SC12816C	✓	✓			✓	
AT88SC25616C	✓	✓			✓	

**Note:** \*Shorter lead times

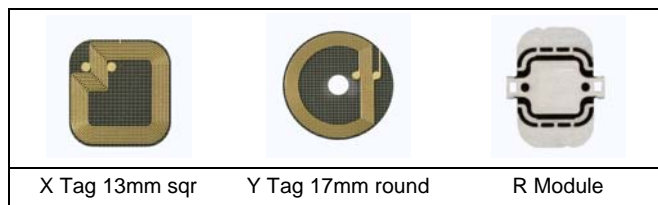
\*\* UDFN (also known as ultra thin mini map)

## CryptoRF Packaging Information



CryptoRF is available in many different shapes and sizes. Specially designed CryptoRF tags in a variety of shapes can be developed for the right business case.

All of our CryptoRF products are available in the standard packages shown below.



## CryptoController (TPM) Packaging Information

Package Type	Catalog No.	Body Size	Pitch	Interface
28 pin TSSOP	AT97SC3204-X1A150	4.4mmx9.7mm	0.65mm	LPC
28 pin TSSOP	AT97SC3204-X1A50	6.1mmx9.7mm	0.65mm	LPC
40 pin QFN	AT97SC3204-X1M50	6.0mm square	0.50mm	LPC
28 pin TSSOP	AT97SC3204T-X1A180	4.4mmx9.7mm	0.65mm	TWI
28 pin TSSOP	AT97SC3204T-X1A80	6.1mmx9.7mm	0.65mm	TWI
40 pin QFN	AT97SC3204T-X1M80	6.0mm square	0.50mm	TWI

## CryptoRF Reader Packaging Information

Part No.	QFN, 36 pin, 6.0mm square
AT88RF1354	✓

## CryptoCompanion Packaging Information

Part No.	SOIC, 8-lead
AT88SC018	✓

# Documentation

## Datasheets

### *CryptoAuthentication*

Devices	Preliminary	Summary	Full Version	Last Update
AT88SA102S	✓			03/2009
AT88SA10HS	✓			06/2009
AT88SA100S	✓			06/2009

### *CryptoMemory*

Devices	Preliminary	Summary	Full Version	Last Update
AT88SCXXXC			✓	04/2009
AT88SC0104CA		✓	✓	05/2009
AT88SC0104C		✓	✓	04/2007
AT88SC0204CA		✓	✓	05/2009
AT88SC0204C		✓	✓	04/2007
AT88SC0404CA		✓	✓	05/2009
AT88SC0404C		✓	✓	04/2007
AT88SC0808CA		✓	✓	05/2009
AT88SC0808C		✓	✓	04/2007
AT88SC1616C		✓	✓	04/2007
AT88SC3216C		✓	✓	04/2007
AT88SC6416C		✓	✓	04/2007
AT88SC12816C		✓	✓	04/2007
AT88SC25616C		✓	✓	04/2007

### *CryptoRF*

Devices	Preliminary	Summary	Full Version	Last Update
AT88SC04C		✓	✓	03/2009
AT88SC0104CRF		✓	✓	03/2009
AT88SC0204CRF		✓	✓	03/2009
AT88SC0404CRF		✓	✓	03/2009
AT88SC0808CRF		✓	✓	03/2009
AT88SC1616CRF		✓	✓	03/2009
AT88SC3216CRF		✓	✓	03/2009
AT88SC6416CRF		✓	✓	03/2009

### ***CryptoRF Reader***

Devices	Preliminary	Summary	Full Version	Last Update
AT88RF1354 (reader chip)	✓			10/2008

### ***CryptoCompanion***

Devices	Preliminary	Summary	Full Version	Last Update
AT88SC018		✓	✓	01/2009

### ***CryptoController***

Devices	Preliminary	Summary	Full Version	Last Update
AT97SC3204		✓	✓	10/2008
AT97SC3204T	✓	✓		10/2008

## Application Notes

### CryptoAuthentication

Name	Description
CryptoAuthentication™ Product Uses	This document provides an introduction to the Atmel AT88SA102 authentication device. This exceptional device enables solutions to countless problems across many industries. The use cases outlined in this document will provide a brief description of possible applications for the AT88SA102 device and how they can be implemented
High Level Security Models	Describes different architectures used in securing applications, including the benefits and drawbacks of choosing a specific model. Developers should be able to choose the appropriate architecture for a common project, or modify one of the architectural models in the document for a special application.
Hardware Reference Design	Provides readers with an overview of the hardware circuitry recommended for deploying the CryptoAuthentication™ chip in various configurations. The document also contains a full description of (Rhino+) Atmel's CryptoAuthentication Demo/Eval board.
High Quality Battery Authentication	This document provides readers with an overview of the Atmel AT88SA100S CryptoAuthentication™ IC. It describe how the AT88SA100S features will provide a solution to prevent counterfeiters from producing batteries that can cause damage to a manufacturers device, a manufacturer's reputations, and/or reduce their potential revenue stream.

### CryptoMemory and CryptoRF

Name	Description
Initializing the CryptoMemory Device for Smartcard Applications	The process of organizing data and determining security settings for the CryptoMemory device. The proper sequence for writing to CryptoMemory is also described.
Programming the CryptoMemory Device for Embedded Applications	CryptoMemory in plastic packages has many security uses in embedded applications. This note describes the process of setting up and programming the CryptoMemory device for such applications.
Understanding the Requirements of ISO/IEC 14443 Type B proximity contactless identification card	Summarizing the signaling and communication protocol requirements for type B contactless smart cards in a tutorial format. The anti-collision protocol implemented in Atmel's Secure RF Smart Card ICs is explained in detail.
Fast Prototyping of a Contactless Reader for CryptoRF	Setting up a complete secure RFID system using Atmel's AT90USBKey development board, CryptoRF tags and the Melexis RF front-end interface.
Using CryptoMemory in Full I <sup>2</sup> C Compliant Mode	Describes how to communicate with CryptoMemory® devices in full I <sup>2</sup> C compliant mode. Full I <sup>2</sup> C compliance permits use of I <sup>2</sup> C hardware peripheral controllers within microcontrollers to communicate with CryptoMemory, thus eliminating the need for software drivers and General Purpose Input/Output (GPIO) pins. This leads to performance improvement by lowering CPU utilization and firmware footprint.

## White Papers

### CryptoAuthentication

Name	Description
256 Bit Key – Is It Big Enough?	This paper address the use of cryptography for the purpose of product authentication, whether it be a physical item or a logical block of firmware, and the key size necessary to be confident that it will not be guessed.

### CryptoMemory and CryptoRF

Name	Description
Understanding CryptoMemory	Atmel's secure serial EEPROM solution making it easy to upgrade from an open EEPROM to a secure solution for embedded applications.
Protecting System Configuration with CryptoMemory	How to use CryptoMemory in an embedded system to store confidential configuration data.
Powerful Security at a Low Cost	Many systems and products need to combat piracy or securely store information, secure Microcontrollers satisfy this need at a high cost characterized by presence of unneeded features. CryptoMemory® provides a low-cost alternative solution that focuses mainly on security.
Using RFID to Stop Counterfeiting	RFID technology is well known for providing labeling solutions to automate inventory control. It is less known for its capability to offer anti-counterfeiting solutions. While providing cryptographic authentication schemes with data protection capabilities, a well-implemented RFID security solution provides complete product protection against illegal cloning, intellectual property theft, and denial-of-service attacks.
Product Counterfeiting Made Easy and Why it is so Difficult to Prevent	The value of the seized counterfeit goods in 2007 is estimated to be over \$600 billion, according to The International Chamber of Commerce (ICC) <sup>1</sup> . Goods that are most frequently counterfeited include computer software, DVDs, CDs, perfume, athletic shoes, drugs, fashion accessories and money orders. Counterfeiting can also involve the theft of valuable intellectual property in electronic systems, such as GPS correlator algorithms or the software that embodies the feature set of a cell phone, GPS or MP3 players.

### CryptoCompanion

Name	Description
Securing Host Side Configuration	There is a growing need for strong hardware security devices in digital systems today. The level of intellectual property or engineering expertise contained within a product continues to grow and as a result it becomes increasingly imperative for the manufacturer to prevent competitors from fraudulently using that IP to obtain a portion of the revenue stream without the associated development cost.

### CryptoController

Name	Description
TPM Decoupling Guidance Application Note	Effective decoupling of the power supply inputs to the TPM is critical to assuring reliable component performance in a high-density printed circuit board environment. This application note provides guidelines which are consistent with industry-standard decoupling recommendations for all active system components.
PC TPM Manufacturing Configuration Application Note	Provides example of TPM configuration during PC system manufacturing.

# Ordering Information

## CryptoAuthentication

Part No.	Pkg Type	Material Description
AT88SA102S	TS	3-pin SOT23, IND Temp Green
AT88SA10HS	TS	3-pin SOT23, IND Temp Green
AT88SA100S	TS	3-pin SOT23, IND Temp Green

**Note:** \*CryptoAuthentication DVS part numbers for quotes and opportunities in Model N are AT88SA102S-DTSU-T, AT88SA10HS-DTSU-T, and AT88SA100S-DTSU-T.

## CryptoMemory

Part No.	Pkg Type	Material Description
AT88SC0104CA	SU	8 SOIC, IND Temp, Green
	TH	8 TSSOP, 4.4mm, IND Temp, Green
	Y6H	8 Contacts, UDFN, IND Temp, Green
	PU	8 PDIP, IND Temp, Green
	MJ	Module J, Green
	WI	Wafer, 150mm not sawn
AT88SC0104C	SU	8 SOIC, IND Temp, Green
	PU	8 PDIP, IND Temp, Green
	MJ	Module J, Green
	WI	Wafer, 150mm not sawn
AT88SC0204CA	SU	8 SOIC, IND Temp, Green
	TH	8 TSSOP, 4.4mm, IND Temp, Green
	Y6H	8 Contacts, UDFN, IND Temp, Green
	PU	8 PDIP, IND Temp, Green
	MJ	Module J, Green
	WI	Wafer, 150mm not sawn
AT88SC0204C	SU	8 SOIC, IND Temp, Green
	PU	8 PDIP, IND Temp, Green
	MJ	Module J, Green
	WI	Wafer, 150mm not sawn
AT88SC0404CA	SU	8 SOIC, IND Temp, Green
	TH	8 TSSOP, 4.4mm, IND Temp, Green
	Y6H	8 Contacts, UDFN, IND Temp, Green
	PU	8 PDIP, IND Temp, Green
	MJ	Module J, Green
	WI	Wafer, 150mm not sawn

**CryptoMemory continued...**

Part No.	Pkg Type	Material Description
AT88SC0404C	SU	8 SOIC, IND Temp, Green
	PU	8 PDIP, IND Temp, Green
	MJ	Module J, Green
	WI	Wafer, 150mm not sawn
AT88SC0808CA	SU	8 SOIC, IND Temp, Green
	TH	8 TSSOP, 4.4mm, IND Temp, Green
	Y6H	8 Contacts, UDFN, IND Temp, Green
	PU	8 PDIP, IND Temp, Green
	MJ	Module J, Green
AT88SC0808C	WI	Wafer, 150mm not sawn
	SU	8 SOIC, IND Temp, Green
	PU	8 PDIP, IND Temp, Green
	MJ	Module J, Green
AT88SC1616C	WI	Wafer, 150mm not sawn
	SU	8 SOIC, IND Temp, Green
	PU	8 PDIP, IND Temp, Green
	MJ	Module J, Green
AT88SC3216C	WI	Wafer, 150mm not sawn
	SU	8 SOIC, IND Temp, Green
	PU	8 PDIP, IND Temp, Green
	MJ	Module J
AT88SC6416C	WI	Wafer, 150mm not sawn
	SU	8 SOIC, IND Temp, Green
	PU	8 PDIP, IND Temp, Green
	MJ	Module J, Green
AT88SC12816C	WI	Wafer, 150mm not sawn
	SU	8 SOIC, IND Temp, Green
	PU	8 PDIP, IND Temp, Green
	MJ	Module J, Green
AT88SC25616C	WI	Wafer, 150mm not sawn
	SU	8 SOIC, IND Temp, Green
	PU	8 PDIP, IND Temp, Green
	MJ	Module J, Green

## CryptoRF

Part No.	Pkg Type	Material Description
AT88RF04C	MX1	13mm Square RFID tag, 35mm tape, body thickness 1mm
	MY1	17mm Round RFID tag, 35mm tape, body thickness 1mm
	MR1	XOA2 Style Smartcard Module
	WA1	6 mil Wafer, 150 mm, Not Sawn
AT88SC0104CRF	MX1	13 mm Square RFID tag, 35mm tape, body thickness 1mm
	MY1	17 mm Round RFID tag, 35mm tape, body thickness 1mm
	MR1	XOA2 Style Smartcard Module
	WA1	6 mil Wafer, 150 mm, Not Sawn
AT88SC0204CRF	MX1	13 mm Square RFID tag, 35mm tape, body thickness 1mm
	MY1	17 mm Round RFID tag, 35mm tape, body thickness 1mm
	MR1	XOA2 Style Smartcard Module
	WA1	6 mil Wafer, 150 mm, Not Sawn
AT88SC0404CRF	MX1	13 mm Square RFID tag, 35mm tape, body thickness 1mm
	MY1	17 mm Round RFID tag, 35mm tape, body thickness 1mm
	MR1	XOA2 Style Smartcard Module
	WA1	6 mil Wafer, 150 mm, Not Sawn
AT88SC0808CRF	MX1	13 mm Square RFID tag, 35mm tape, body thickness 1mm
	MY1	17 mm Round RFID tag, 35mm tape, body thickness 1mm
	MR1	XOA2 Style Smartcard Module
	WA1	6 mil Wafer, 150 mm, Not Sawn
AT88SC1616CRF	MX1	13 mm Square RFID tag, 35mm tape, body thickness 1mm
	MY1	17 mm Round RFID tag, 35mm tape, body thickness 1mm
	MR1	XOA2 Style Smartcard Module
	WA1	6 mil Wafer, 150 mm, Not Sawn
AT88SC3216CRF	MX1	13 mm Square RFID tag, 35mm tape, body thickness 1mm
	MY1	17 mm Round RFID tag, 35mm tape, body thickness 1mm
	MR1	XOA2 Style Smartcard Module
	WA1	6 mil Wafer, 150 mm, Not Sawn
AT88SC6416CRF	MX1	13 mm Square RFID tag, 35mm tape, body thickness 1mm
	MY1	17 mm Round RFID tag, 35mm tape, body thickness 1mm
	MR1	XOA2 Style Smartcard Module
	WA1	6 mil Wafer, 150 mm, Not Sawn

## CryptoRF Reader

Part No.	Pkg Type	Material Description
AT88RF1354	ZU	6 x 6 mm QFN, 36 Pins, Bulk
	ZU-T	6 x 6 mm QFN, 36 Pins, Tape and Reel

## CryptoCompanion

Part No.	Pkg Type	Material Description
AT88SC018	SX	8 SOIC, RoHS, Commercial Temp, T&R

## CryptoController (TPM)

Part No.	Pkg Type	Material Description
AT97SC3204-X1A150	4.4mm TSSOP	LPC no EK, No Lic. 4.4mm 28-TSSOP
AT97SC3204-X1A50	6.1mm TSSOP	LPC no EK, No Lic., 6.1mm 28-TSSOP
AT97SC3204-X9M50	QFN	LPC no EK, No Lic. 40-QFN
AT97SC3204T-X1A180	4.4mm TSSOP	TWI no EK, No Lic. 4.4mm 28-TSSOP
AT97SC3204T-X1A80	6.1mm TSSOP	TWI no EK, No Lic., 6.1mm 28-TSSOP
AT97SC3203T-X9M80	QFN	TWI no EK, No Lic. 40-QFN

## Kit Ordering Information

### CryptoAuthentication Kits

Part No.	Material Description
AT88SA-ADK1 Rhino+	AVR based demonstration/evaluation kit for the CryptoAuthentication AT88SA102S

### CryptoMemory Kits

Part No.	Material Description
AT88SC-DK1 Aris	Easily add CryptoMemory security to the customer's existing system; can be used with Atmel AVR and ARM starter kits.
AT88SC-ADK2 Aris+	Low-cost development kit for CryptoMemory and CryptoCompanion chips on an AVR platform.

### CryptoRF Kits

Part No.	Material Description
AT88SCRF-ADK2 Keen+	Lowest cost reader reference design; uses Atmel reader IC on an AVR platform
AT88SCRF-ADK1 Yuma+	For secure RFID developers who prefer an AVR platform; Melexis® reader IC
AT88SCRF-S7DK2P CryptoRF/SkyeTek	ARM platform, SkyeTek Reader

### CryptoController Kits

Part No.	Material Description
AT97SC3204T-X1A180	Embedded TPM development kit based on AVR

For contact information, please go to [www.cryptomemory.com](http://www.cryptomemory.com)

