Atmel Crypto Products Portfolio

Family of Secure Authentication Solutions

Atmel Crypto Products Portfolio

The Atmel® Crypto Products Portfolio offers full system security solution options for a wide variety of applications. The Portfolio consists of both client and host hardware security ICs, which provide authentication, encryption and secure data storage capabilities.

Why hardware security? Confidential data or secrets stored by unsecured means, such as in standard memories, are vulnerable to attack and exposure. Hardware security ICs include many sophisticated design features specifically aimed at keeping confidential data and core secrets safe from hackers, thereby protecting corporate revenue, valuable intellectual property and limiting potential liability exposure.

System security is only as strong as the weakest link. This well-known phrase should remain in the forefront of any system developer's mind as they conceptualize a secure system design. Many systems today are deployed with a hardware security solution on the client side, while the host-side secrets are stored in unsecured memories (Figure 1). For those who recognize this host-side implementation as a potential weakness, Atmel offers host-side hardware security companion ICs specifically designed to eliminate this weakness (Figure 2). Crypto Products host companion ICs implement the host algorithm in hardware and securely store and manage the host secrets, thereby strengthening the system-level security and reducing development time.

The Crypto Products Portfolio is ideally suited for a variety of applications, and in some cases more than one product in the Portfolio can provide a solution for a given application. For example, if an application requires both authentication and secure memory storage in a wired environment, Atmel CryptoMemory® may be the best solution. If a contactless interface is desired, Atmel CryptoRF®, along with the supporting Reader IC, is an excellent choice. In cases where the strength of a 256-bit key size is preferred, Atmel CryptoAuthentication™ is the answer. Lastly, when a high security standards-based solution is required, Atmel CryptoController™ (TPM) is a great choice.

Applications

- Authentication
- IP protection
  - Encrypted software downloads
  - Software and media antipiracy
  - Firmware copy prevention
- System integrity
- Secure communication
- Physical, network and computer access control
- Secure key exchange

Markets

- Metering
- GPS
- Printers
- Set top boxes
- Portable media players
- Anti-cloning of consumables
  - Filters
  - Cartridges
  - Chemical reagents
  - Batteries
- PDA/Cell phones
- Medical devices
- E-purse

Figure 1. Client only hardware security

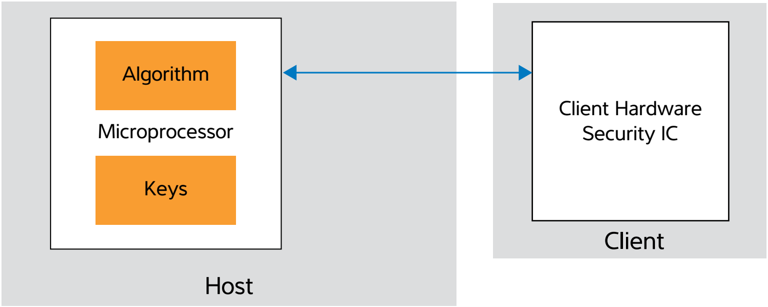
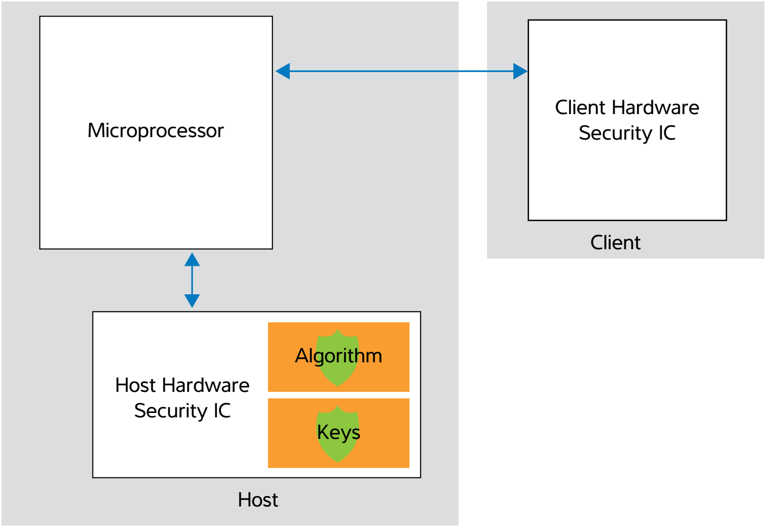


Figure 2. Client and host hardware security

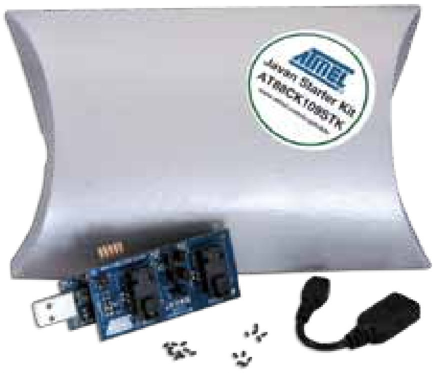


Atmel Crypto Authentication

Atmel® CryptoAuthentication™ is the first family of secure authentication ICs using the SHA-256 hash algorithm with a 256-bit key length, providing robust hardware authentication at a very cost-effective price. With CryptoAuthentication, Atmel ATSHA204 developers can easily implement secure authentication and validation of physical or logical elements in virtually all microprocessor-based systems using the straightforward 256-bit challenge/response protocol. It is ideal for handheld electronic systems or any embedded system where space is at a premium with features such as a tiny 3-pin SOT23 package and a single-wire interface.

Implementing host side security to provide a full system solution is now easier than ever. The Atmel ATSHA204 includes both client and host security capability, offloading key storage and the execution algorithms from the MCU, significantly reducing both system cost and complexity. When using the Atmel ATSHA204 on the host, systems designers no longer need to worry about the cryptographic algorithms for their systems.

Figure 3. Atmel AT88CK109STK8 starter kit



Key Features

- Secure authentication and key exchange
- Superior SHA-256 hash algorithm
- Best-in-class 256-bit key length
- Guaranteed unique serial number
- High-speed I^{2}C and single-wire interface options
- 1.8 – 5.5V communications
- 4-Kbit EEPROM for key and data storage
- <100nA sleep current
- Multi-level hardware security
- Secure personalization
- Green compliant (exceeds RoHS) plastic packages

Advantages

- High-security authentication at the lowest total system cost
  - Single-wire interface reduces connector cost and requires fewer GPIO pins
  - Sophisticated hardware security features
- Fits in the smallest systems
  - Tiny 3-pin SOT23 is ideal for hand-held systems
- Quick time-to-market
  - ATSHA204 includes both client and host device capability, eliminating the need to write, debug or test system crypto code
  - Can be used with any microprocessor

Atmel Device	Description	Interface	Temp	V_{CC}
ATSHA204	Client/Host Authentication with EEPROM	I^{2}C / Single Wire	-40°C to 85°C	2.0-5.5V
AT88SA102S	Secure Authentication	Single Wire	-40°C to 85°C	2.5-5.5V
AT88SA10HS	Host-side Authentication	Single Wire	-40°C to 85°C	2.5-5.5V

Package Options

- 3-pin SOT23 (1.3mm x 2.9mm body)
- 8-lead SOIC
- 8-lead TSSOP

Development Kits*

- Atmel AT88CK454BLACK – Evaluation Kit
- Atmel AT88CK101STK8 – Starter Kit
- Atmel AT88CK109STK8 – Starter Kit
- Atmel ATAVRSECURITYX – Atmel AVR® Xplained Add-on Board

*See Page 6 for full description

Atmel CryptoRF

World´s Largest Family of Secure RF Memories

The Atmel® CryptoRF® Transponder and Atmel CryptoRF Reader Pair offer a full RFID secure authentication solution for embedded and non-embedded applications. CryptoRF is a 13.56MHz RFID device family with a 64-bit embedded hardware encryption engine, mutual authentication capability and up to 64-Kbit of user memory. CryptoRF is ideally suited to meet a variety of security applications such as product authentication, contactless payment, patient safety, anti-cloning of consumables, loyalty 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 is compatible with the Atmel CryptoCompanion™ which provides plug and play host-side cryptographic security.

Atmel Device	Description	Zones	Package	Interface
AT88RF04C	4-Kbit Secure RFID	4	Tags, Modules, Wafers	IS014443 Type B
AT88SC0808CRF	8-Kbit Secure RFID	8	Tags, Modules, Wafers	IS014443 Type B
AT88SC1616CRF	16-Kbit Secure RFID	16	Tags, Modules, Wafers	IS014443 Type B
AT88SC3216CRF	32-Kbit Secure RFID	16	Tags, Modules, Wafers	IS014443 Type B
AT88SC6416CRF	64-Kbit Secure RFID	16	Tags, Modules, Wafers	IS014443 Type B
AT88RF1354	ISO 14443 Type B Reader	–	36-lead QFN	2-wire + SPI
AT88SC018	Host-side Security	–	8-lead SOIC	2-wire

Key Features

- 64-bit mutual authentication protocol
- Stream encryption ensuring data privacy
- Multiple key sets for authentication and encryption
- Cryptographic message authentication codes (MAC)
- Encrypted passwords with attempt counters
- Selectable access rights by zone
- Tamper sensors
- Compliant with industry standards

Package Options

CryptoRF is available in many different shapes and sizes. Specially designed CryptoRF tags in a variety of shapes can be developed for high volume applications.

- Epoxy glass tags
  - 13.0mm x 13.0mm
  - 17.0mm round
  - 8.6mm x 18.1mm
- Polyethylene Terephthalate (PET) tag
  - 20.0mm x 20.0mm
- Industry standard modules

Advantages

- Full Atmel system solution
- No operating system needed; easy to program
- Flexible independently configurable user memory zones
- Fast time-to-market
  - Interface software available for easy implementation
- Rich set of security features
- Flexible security options

Development Kits*

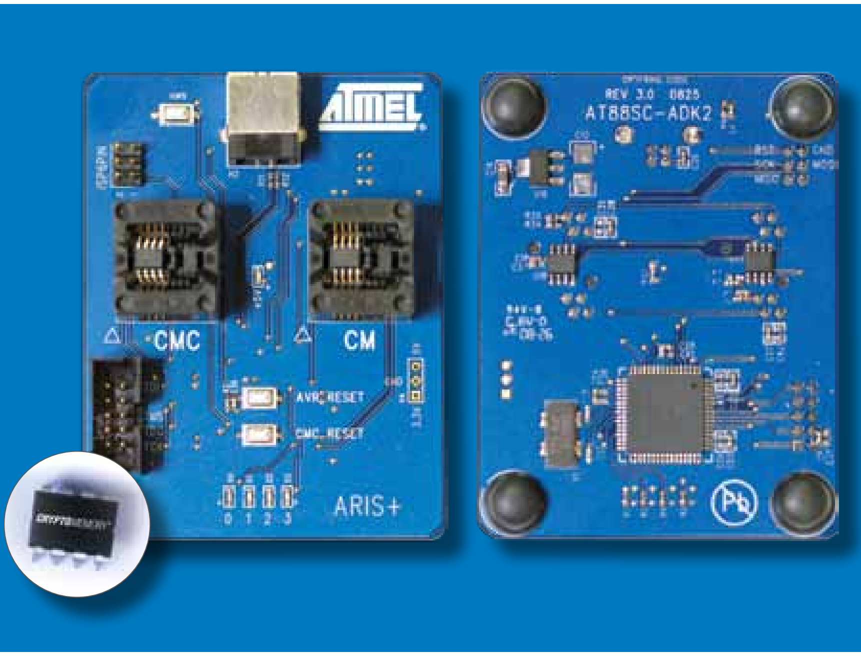
- Atmel AT88CK201STK – Starter Kit

*See Page 6 for full description

Atmel CryptoMemory

The World's Only Secure Serial EEPROM
Atmel® CryptoMemory® cryptographic security ICs offer a cost-efficient, high-security solution for any application requiring authentication, data protection or secure storage.

A cryptographic algorithm encrypts data and passwords, generates Message Authentication Codes (MAC) thereby providing a secure place where information remains safe, even under attack. CryptoMemory is the only family of secure memory devices in the industry with mutual authentication between device and host, plus data encryption. Both synchronous (2-wire) and asynchronous (ISO7816) protocols are available.



Key Features

- A family of devices with user memories from 1-Kbit to 256-Kbit
- Symmetrical dynamic mutual authentication with 64-bit cryptographic keys
- Encrypted passwords with attempt counters
- Stream encryption ensures data privacy
- 1.0MHz compatible 2-wire serial interface for fast operation
- Pin compatible with industry standard 24Cxxx serial memories

Advantages

- No operating system required; easy to program
- Flexible, independently configurable user memory zones
- Fast time-to-market
  - Interface software available for easy implementation
- Rich set of security features
- Flexible security options

Package Options

- Plastic Packages
  - 8-lead SOIC
  - 8-lead PDIP
  - 8-lead TSSOP
  - 8-lead uDFN (Ultra Thin Mini-MAP)
- Modules

Development Kits*

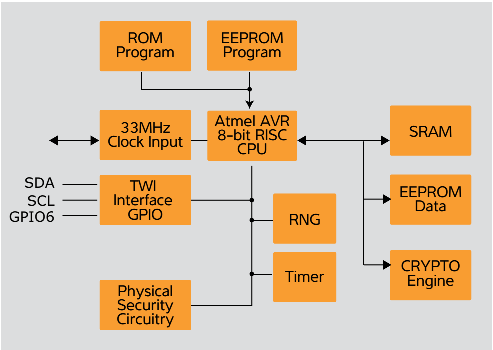
- Atmel AT88SC-ADK2 – Starter Kit

*See Page 6 for full description

Atmel Device	Description	Zones	Temp	V_{CC}
AT88SC0104CA	1-Kbit Secure EEPROM	4	-40°C to 85°C	2.7 to 3.6V
AT88SC0204CA	2-Kbit Secure EEPROM	4	-40°C to 85°C	2.7 to 3.6V
AT88SC0404CA	4-Kbit Secure EEPROM	4	-40°C to 85°C	2.7 to 3.6V
AT88SC0808CA	8-Kbit Secure EEPROM	8	-40°C to 85°C	2.7 to 3.6V
AT88SC1616C	16-Kbit Secure EEPROM	16	-40°C to 85°C	2.7 to 5.5V
AT88SC3216C	32-Kbit Secure EEPROM	16	-40°C to 85°C	2.7 to 5.5V
AT88SC6416C	64-Kbit Secure EEPROM	16	-40°C to 85°C	2.7 to 5.5V
AT88SC12816C	128-Kbit Secure EEPROM	16	-40°C to 85°C	2.7 to 5.5V
AT88SC25616C	256-Kbit Secure EEPROM	16	-40°C to 85°C	2.7 to 5.5V
AT88SC018	Host Side Security	–	-40°C to 85°C	2.7 to 3.6V

Atmel CryptoController (TPM)

Atmel® CryptoController™ is a complete turnkey Trusted Platform Module (TPM) 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 the Atmel AVR® microcontrollers 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 standards-based solution for all computing devices.



Atmel Device	Description	Temp	V_{CC}
AT97SC3204	LPC	0°C to 70°C, and -40°C to 85°C	3.0V to 3.6V
AT97SC3204T	TWI	0°C to 70°C, and -40°C to 85°C	3.0V to 3.6V

Key Features

Based on the Atmel AVR 8-bit RISC CPU

- Full Trusted Computing Group (TCG) v1.2 specification compliant
- 2048-bit Hardware RSA Crypto Accelerator
- Hardware SHA-1 Accelerator, 50μs/64-byte block
- On-chip storage of up to 21 user keys
- Reliable EEPROM for nonvolatile storage, no batteries required
- True Hardware random number generator

Package Options

- 28-lead TSSOP
- 40-lead QFN

Advantages

- Standards based security
- Available in industrial grade
- AVR 8-bit core
- Tools for embedded development

Applications

- IP protection
- System integrity
- Authentication
- Secure communication

Markets

- Multifunction printers
- Networks
- Gaming (entertainment /gambling)
- Set-top boxes
- PCs
- Servers
- PDAs/pocket PCs
- Femto cells

Development Kits*

- Atmel AT97SC3204T-X1K180 - Embedded Development Kit
- Atmel AT97SC3204-X1DB190 - PC Evaluation Daughter Board

*See Page 6 for full description

Tools and Support

Atmel CryptoAuthentication Kits

Evaluation Kit – Atmel® AT88CK454BLACK
Includes a low cost USB dongle board for demonstrating the functionality of the Atmel CryptoAuthentication™ ATSHA204 device. Software tools and libraries available at www.atmel.com

Single Socket Starter Kit – Atmel AT88CK101STK8
Includes a single socket board for client development, an Atmel AVR® microbase board, USB extension cable and samples of the ATSHA204 device. Designed to be used with the Atmel STK500/STK600 development kits or as a stand-alone kit via USB connectivity. Software tools and libraries available at www.atmel.com

Dual Socket Starter Kit – Atmel AT88CK109STK8
Includes a dual-socket board for client or client/host development, an Atmel AVR microbase board, USB extension cable, and samples of the Atmel ATSHA204 device. Designed to be used with the Atmel STK500/STK600 development kits or as a stand-alone kit via USB connectivity. Software tools and libraries available at www.atmel.com

Security Xplained – Atmel ATAVRSECURITYX
Security Xplained is an add-on board for the Atmel AVR Xplained series that adds security functionality. Security Xplained is ASF library supported and demonstrates how the Atmel ATSHA204 device requires only a very simple circuit design and minimal external components to add security to any system. Software tools and libraries available at www.atmel.com

Atmel CryptoMemory Kits

Starter Kit – Atmel AT88SC-ADK2
Includes a dual socket board for Atmel CryptoMemory® and Atmel CryptoCompanion™ development on an Atmel AVR platform, USB cable, and samples of CryptoMemory and CryptoCompanion devices. Software tools and libraries available at www.atmel.com

Atmel CryptoRF Kits

Starter Kit – Atmel AT88CK201STK
Includes a reader board for Atmel CryptoRF® development, an AT88Microbase AVR board, USB cable and samples of CryptoRF tags. Software tools and libraries available at www.atmel.com

Atmel CryptoController Kits

Embedded Development Kit – Atmel AT97SC3204T-X1K180
Based on the Atmel AVR AT90USBKey kit with an added Embedded TWI (2-wire) TPM card and Embedded TWI TPM demonstration and evaluation software. The kit includes TPM TWI module, Atmel AT90USBKey, USB adapter cables, USB flash drive with sample code and documentation and an alternate 9V battery supply cable.

PC Evaluation Daughter Board – Atmel AT97SC3204-X1DB190
This compact daughter board is designed to provide a simple PC interface to system designers via an industry standard 20-pin header. Includes a daughter board with 20-pin header and a mounted Atmel TCG compliant v1.2 LPC TPM.

For other kit options to support a variety of development needs, visit www.atmel.com

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

Atmel Asia Limited
Unit 01-5 & 16, 19F
BEA Tower, Millennium City 5
418 Kwun Tong Road
Kwun Tong, Kowloon
HONG KONG
Tel: (+852) 2245-6100
Fax: (+852) 2722-1369

Atmel Munich GmbH
Business Campus
Parkring 4
D-85748 Garching b. Munich
GERMANY
Tel: (+49) 89-31970-0
Fax: (+49) 89-3194621

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

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 THE ATMEL TERMS AND CONDITIONS OF SALES LOCATED ON THE ATMEL WEBSITE, 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 AND 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 products 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 products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.