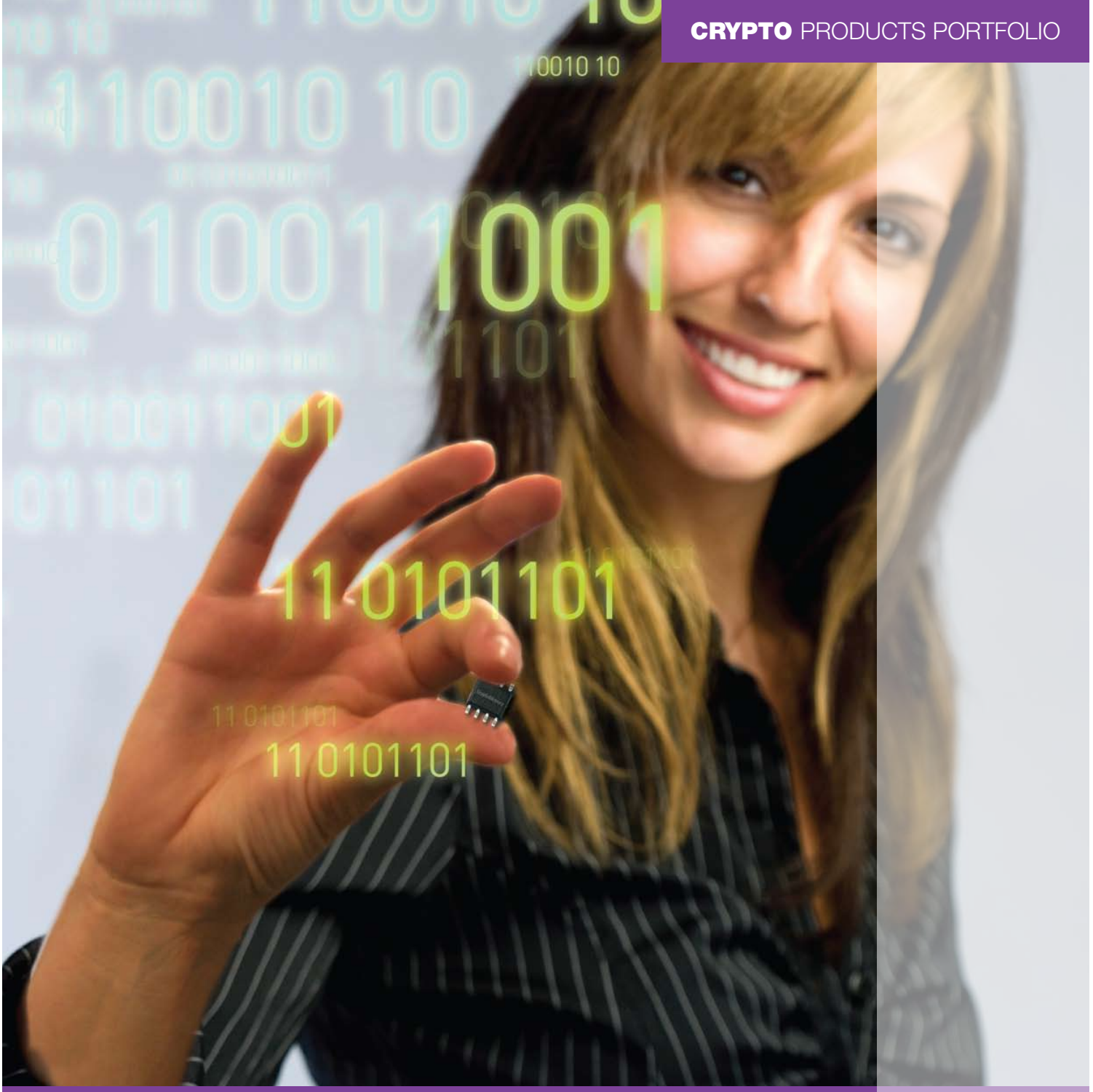


Crypto Products Portfolio

Family of Secure Authentication Solutions

Crypto Products Overview

Atmel®'s Crypto Products portfolio offers full system security solution options for a wide variety of applications. The family consists of both client and host hardware security ICs, which provide authentication, encryption, and secure data storage capabilities (figure 1).

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, protecting valuable intellectual property, and limiting potential liability exposure.

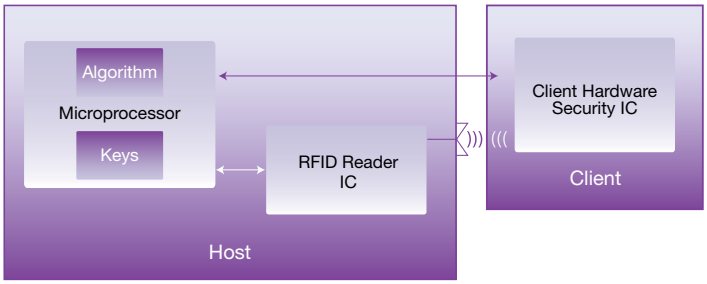
System security is only as strong as the weakest link. This well known phrase should remain in the forefront of any system developers mind as they conceptualize a secure system design. Many systems today are deployed with a hardware security solution on the client side, while the host-side secrets are stored in unsecured memories. 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 family is ideally suited for a variety of applications, and in some cases more than one product in the family can provide a solution for a given application. For example, if an application requires both authentication and secure memory storage in a wired environment, CryptoMemory® may be the best solution. If a contact-less interface is desired, CryptoRF®, along with the supporting Reader IC, is an excellent choice. In cases where the strength of a 256 bit key size is preferred, CryptoAuthentication™ is the answer. Lastly, when a high security standards-based solution is required, CryptoController™ (TPM) is a great choice. Application and market possibilities for Crypto Products include:

Applications

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

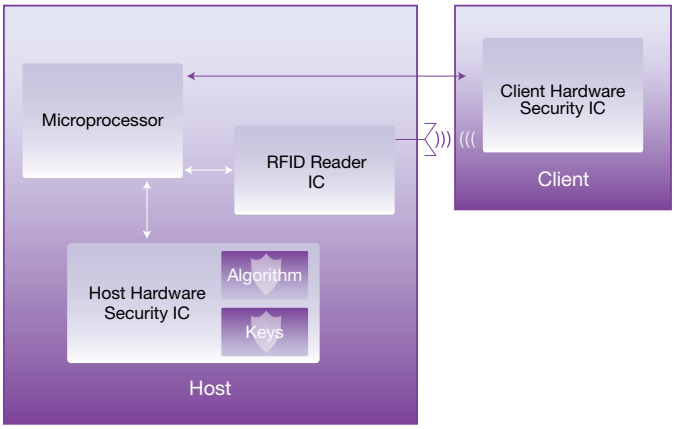
Figure 1



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 2



CryptoAuthentication™

CryptoAuthentication is Atmel's 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 AT88SA102S and AT88SA100S 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 a premium with features such as a tiny 3-pin SOT23 package and a single wire interface.

Implementing CryptoAuthentication's host side IC provides a full system solution. The host chip off-loads key storage and the execution algorithms, significantly reducing both system cost and complexity. When using the host IC, systems designers no longer need to develop the cryptographic algorithms for their systems.

Device	Description	Interface	Temp	VCC
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
AT88SA100S	Battery Authentication	Single Wire	-40°C to 85°C	2.5-5.5V

Key Features

- Secure authentication & key exchange
- Superior SHA-256 hash algorithm
- Best in class 256 bit key length
- Guaranteed unique serial number
- High speed single wire interface
- 1.8 – 5.5V communications
- <100nA sleep current
- Multi-level hardware security
- Secure personalization
- Green compliant (exceeds RoHS) 3 pin SOT-23 package
- Keys stored in battery backed SRAM – AT88SA100S only

Advantages

- High security authentication at 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
  - AT88SA10HS host device eliminates need to write, debug or test system crypto code
  - Can be used with any microprocessor

Packaging

- CryptoAuthentication is available in a 3-pin SOT23 (1.3mm x 2.9mm body)

Development Kits*

- AT88CK109STK3 – Starter Kit
- AT88SA-ADK1 – Evaluation Kit.

*See Page 7 for full description.

AT88CK109STK3 Starter Kit

CryptoRF®

World's Largest Family of Secure RF Memories

The CryptoRF transponder and CryptoRF reader pair offer a full RFID secure authentication solution for embedded and non-embedded applications. CryptoRF is a 13.56 MHz 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 Atmel's CryptoCompanion which provides plug and play host-side cryptographic security.

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	S014443 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

CRYPTORF®

Packaging

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*

- AT88CK201STK – Starter Kit

*See Page 7 for full description.

CryptoMemory®

The World's Only Secure Serial EEPROM

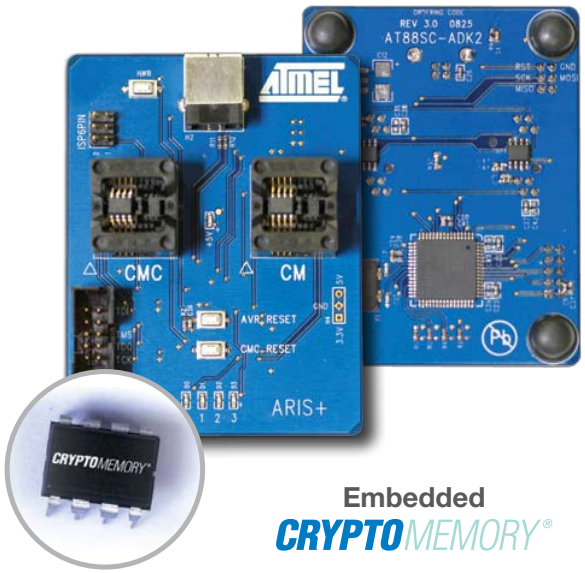
CryptoMemory cryptographic security ICs offer a cost efficient, high security solution for any application requiring authentication, data protection, or secure storage.

A cryptographic algorithm encrypts data and passwords, and 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.

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

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
- 1.0 MHz compatible 2-wire serial interface for fast operation
- Pin compatible with industry standard 24CXX Serial Memories



Embedded CRYPTOMEMORY®

Advantages

- 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

Circuits are available in a variety of packages

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

Development Kits*

- AT88SC-ADK2 – Starter Kit

*See Page 7 for full description.

CryptoController™ (TPM)

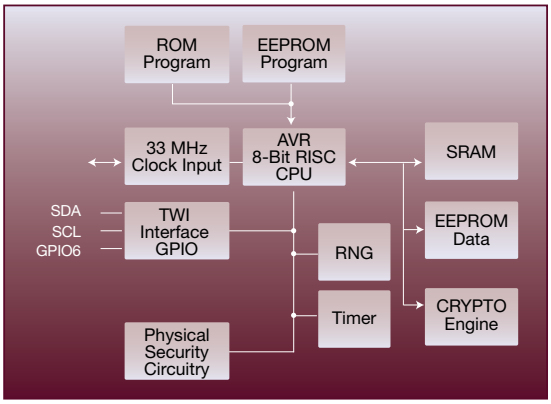
CryptoController, Atmel's embedded Trusted Platform Module. TPM is a complete turnkey solution providing ultra-strong security for both PC and embedded systems. Primary TPM capabilities include IP protection, system integrity, authentication, and secure communication. The core building blocks in CryptoController 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 standards based solution for all computing devices.

Device	Interface	Temp	VCC
AT97SC3204	LPC	0°C to 70°C, and -40°C to 85°C	3.0-3.6V
AT97SC3204T	TWI	0°C to 70°C, and -40°C to 85°C	3.0-3.6V

Key Features

Based on Atmel's 8-Bit AVR RISC CPU

- Full Trusted Computing Group (TCG) v1.2 specification compliant
- 2048 bit Hardware RSA Crypto Accelerator
- Hardware SHA-1 Accelerator, 50 µs / 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



Applications

- IP protection
- System integrity
- Authentication
- Secure communication

Advantages

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

Packaging

- 28-lead TSSOP and 40-lead QFN packages available

Markets

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

Development Kits*

- AT97SC3204T-X1K180 - Embedded Development Kit
- AT97SC3204-X1DB150 - PC evaluation daughter board

*See Page 7 for full description.

Tools and Support

CryptoAuthentication Kits:

Evaluation Kit – AT88SA-ADK1 – Includes a low cost USB dongle board for demonstrating the functionality of the AT88SA102S CryptoAuthentication device. Software tools and libraries available at www.atmel.com.

Starter Kit – AT88CK109STK3 – Includes a dual socket board for Client or Client/Host development, an AT88Microbase AVR board, USB extension cable, and samples of the AT88SA10xS family of CryptoAuthentication devices. Software tools and libraries available at www.atmel.com.

CryptoMemory Kits:

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

CryptoRF Kits:

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

CryptoController Kits:

Embedded Development Kit – AT97SC3204T-X1K180 – Based on the 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, AT90USBKey, USB adapter cables, USB flash drive with sample code & documentation, and an alternate 9V battery supply cable.

PC Evaluation Daughter Board – AT97SC3204-X1DB150 – 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, please visit www.atmel.com

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

Regional Headquarters
Europe
Atmel Sarl
Route des Arsenaux 41
Case postale 80
CH-1705 Fribourg
Switzerland
Tel: (41) 26-426-5555
Fax: (41) 26-426-5500

Asia
Room 1219
Chinachem Golden Plaza
77 Mody Road Tsimshatsui
East Kowloon
Hong Kong
Tel: (852) 2721-9778
Fax: (852) 2722-1369

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 Information:
Avenue de Rochepleine
BP 123
38521 Saint Egrève Cedex
France
Tel: (33) 4-76-58-47-50
Fax: (33) 4-76-58-47-60

Literature request
www.atmel.com/literature

Web Site
www.atmel.com

8705A-11/09-500