Atmel CryptoAuthentication™
Family of Hardware Security Solutions
ATSHA204 and ATAES132

The Atmel® ATSHA204 is the first member of the CryptoAuthentication™ family of secure authentication ICs to integrate the SHA-256 hash algorithm with a 4.5-Kbit EEPROM, providing robust hardware authentication and secure key/data storage at a very cost-effective price. With the 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 small outline plastic packages and a single-wire interface. Implementing host-side security to provide a full system solution is now easier than ever. The Atmel ATSHA204 includes 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 writing crypto algorithms or developing crypto protocols for their systems.

Key Features and Benefits

- Multi-level hardware security
- Secure authentication and key exchange
- Superior SHA-256 hash algorithm
- Best-in-class, 256-bit key length
- High-quality hardware random number generator
- Guaranteed unique serial number
- 4.5-Kbit EEPROM for key and data storage
- High-speed I2C and single-wire interface options
- 1.8 – 5.5V communications
- < 150nA sleep current
- Secure personalization
- Green compliant plastic packages

Advantages

- High-security authentication at the lowest total system cost
  - Single-wire interface reduces connector cost and requires fewer GPIO pins
  - I2C interface standard in many microcontroller systems
  - Sophisticated hardware security features
- Fits in smallest systems
  - Available small package outlines 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

Product Availability and Ordering Information

Atmel Ordering Code	Voltage Range	Interface	Package	Samples Availability
ATSHA204-TSU-T	2.0 – 5.5V	single-wire	SOT23 3	Now
ATSHA204-SH-CZ-T	2.0 – 5.5V	single-wire	SOIC 8	Now
ATSHA204-TH-CZ-T	2.0 – 5.5V	single-wire	TSSOP 8	Now
ATSHA204-MAH-CZ-T	2.0 – 5.5V	single-wire	UDFN 8	Now
ATSHA204-SH-DA-T	2.0 – 5.5V	I²C	SOIC 8	Now
ATSHA204-TH-DA-T	2.0 – 5.5V	I²C	TSSOP 8	Now
ATSHA204-MAH-DA-T	2.0 – 5.5V	I²C	UDFN 8	Now
ATSHA204-RBH-T	2.0 – 5.5V	single-wire	3-lead Contact	Now

Application Examples

- Portable devices and accessories
- Li-ion batteries
- Smart meters
- In-home displays
- Medical devices
- Set-top boxes

Atmel CryptoAuthentication™
Family of Hardware Security Solutions
ATSHA204 and ATAES132

The Atmel® ATAES132 is the latest member of the CryptoAuthentication™ family of secure authentication devices, and utilizes an AES-128 cryptographic engine to provide both authentication and confidential, nonvolatile data storage. The ATAES132 is pin-out and instruction set compatible with standard SPI and I2C serial EEPROMs, allowing system designers to quickly and cost-effectively add security functionality to their products. The 32-Kbit EEPROM is segmented into sixteen user zones, with access permissions independently configured, as well as sixteen 128-bit keys, which can be used with any zone. These keys can also be used for standalone authentication. This key management flexibility makes ATAES132 ideal for a wide variety of applications. The ATAES132 incorporates multiple physical security mechanisms to prevent release of the internally stored secrets, as well as secure personalization features to facilitate third-party product manufacturing.

Key Features and Benefits

- Secure authentication and key exchange
- AES algorithm with 128-bit keys
- AES-CCM for authentication
- High-quality hardware random number generator
- 16 non-reversible, monotonic counters
- Secure storage for sixteen 128-bit keys
- 32-Kbit EEPROM user memory for secure data storage
- 1MHz I2C and 10MHz SPI interface options
- 2.5 – 5.5V supply voltage
- < 250nA sleep current
- Multi-level hardware security
- Secure personalization
- Serial EEPROM fully compatible pin-out
- Green compliant plastic packages

Key Features and Benefits

- High-security authentication using AES
  - Proven algorithm, recommended by cryptographic experts
  - Sophisticated hardware security features
- Fits in smallest systems
  - Available small package outlines ideal for space-constrained systems
- Quick time to market
  - Fully pin-out compatible with standard serial EEPROMs, allowing placement on existing PC boards
  - Flexible, user-configured security
  - Can be used with any microprocessor

Product Availability and Ordering Information

Atmel Ordering Code	Voltage Range	Interface	Package	Samples Availability
ATAES132-SH-ER-T	2.5 – 5.5V	I²C	SOIC 8	Now
ATAES132-TH-ER-T	2.5 – 5.5V	I²C	TSSOP 8	Now
ATAES132-MA3H-ER-T	2.5 – 5.5V	I²C	UDFN 8	Now
ATAES132-SH-EQ-T	2.5 – 5.5V	SPI	SOIC 8	Now
ATAES132-TH-EQ-T	2.5 – 5.5V	SPI	TSSOP 8	Now
ATAES132-MA3H-EQ-T	2.5 – 5.5V	SPI	UDFN 8	Now

Application Examples

- Portable devices and accessories
- Li-ion batteries
- Smart meters
- In-home displays
- Medical devices
- Set-top boxes
- White goods

For more information, visit http://www.atmel.com/MEM_ATSHA204

Atmel | Enabling Unlimited Possibilities®

Atmel Corporation 1600 Technology Drive, San Jose, CA 95110 USA **T :** (+1)(408) 441. 0311 **F :** (+1)(408) 487. 2600 | **www.atmel.com**