Atmel ATAES132

CryptoAuthentication family of hardware security solutions

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 the 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
- Multilevel hardware security
- Secure personalization
- Serial EEPROM fully compatible pin-out
- Green-compliant plastic packages

Advantages

- 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
  - 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

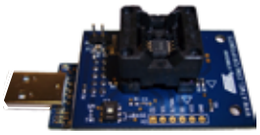
- Portable devices and accessories
- Li-ion batteries
- Smart meters
- In-home displays
- Medical devices
- Set-top boxes
- White goods

Atmel ATAES132

CryptoAuthentication family of hardware security solutions

Integrating hardware security into embedded systems has never been easier than with the Atmel® CryptoAuthentication™ family of hardware security solutions. Multiple evaluation and development support tools are available for the Atmel ATAES132, giving designers the necessary flexibility to meet the most aggressive development timelines. To gain a basic understanding of the Atmel ATAES132 device architecture and capabilities, the very low-cost AT88CK427GREEN demonstration kit is a great choice. For more comprehensive evaluation and development capabilities, designers can choose from client or client and host kit configurations that include USB connectivity as well as a modular hardware design approach that enables rapid and easy development in most development environments. Additionally, the Atmel ATAVRSECURITYX Security Xplained add-on board for the Atmel AVR® Xplained development platform provides a seamless avenue to integrate security into your embedded application. All Atmel ATAES132 tools are based on Atmel AVR devices, with software and libraries available at www.atmel.com.

AT88CK427GREEN



AT88CK101STK8

ATAVRSECURITYX

AT88CK109STK8

Tool Availability and Ordering Information

Atmel Ordering Code	Description	Interface	Package	Samples	Availability
AT88CK427GREEN	USB dongle secure authentication demonstration kit for Atmel ATAES132	I²C	8-lead TSSOP	Yes	Now
AT88CK101STK8	Single-socket secure authentication development kit for Atmel ATAES132	I²C	8-lead SOIC	Yes	Now
AT88CK109STK8	Dual-socket secure authentication development kit for Atmel ATAES132	I²C	8-lead SOIC	Yes	Now
ATAVRSECURITYX	Atmel ATAES132 security add-on board for Atmel AVR Xplained series	I²C	8-lead SOIC	Yes	Now

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