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

<table>
<thead>
<tr>
<th>Atmel Ordering Code</th>
<th>Voltage Range</th>
<th>Interface</th>
<th>Package</th>
<th>Samples Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATAES132-SH-ER-T</td>
<td>2.5 – 5.5V</td>
<td>I²C</td>
<td>SOIC 8</td>
<td>Now</td>
</tr>
<tr>
<td>ATAES132-TH-ER-T</td>
<td>2.5 – 5.5V</td>
<td>I²C</td>
<td>TSSOP 8</td>
<td>Now</td>
</tr>
<tr>
<td>ATAES132-MA3H-ER-T</td>
<td>2.5 – 5.5V</td>
<td>I²C</td>
<td>UDFN 8</td>
<td>Now</td>
</tr>
<tr>
<td>ATAES132-SH-EQ-T</td>
<td>2.5 – 5.5V</td>
<td>SPI</td>
<td>SOIC 8</td>
<td>Now</td>
</tr>
<tr>
<td>ATAES132-TH-EQ-T</td>
<td>2.5 – 5.5V</td>
<td>SPI</td>
<td>TSSOP 8</td>
<td>Now</td>
</tr>
<tr>
<td>ATAES132-MA3H-EQ-T</td>
<td>2.5 – 5.5V</td>
<td>SPI</td>
<td>UDFN 8</td>
<td>Now</td>
</tr>
</tbody>
</table>

Application Examples
- Portable devices and accessories
- Li-ion batteries
- Smart meters
- In-home displays
- Medical devices
- Set-top boxes
- White goods
Atmel Corporation has developed a family of hardware security solutions known as the CryptoAuthentication™ family. These solutions provide a flexible approach to meeting the most aggressive development timelines. The Atmel ATAES132 is a key component in this family.

### Tool Availability and Ordering Information

<table>
<thead>
<tr>
<th>Atmel Ordering Code</th>
<th>Description</th>
<th>Interface</th>
<th>Package</th>
<th>Samples</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT88CK427GREEN</td>
<td>USB dongle secure authentication demonstration kit for Atmel ATAES132</td>
<td>PC</td>
<td>8-lead TSSOP</td>
<td>Yes</td>
<td>Now</td>
</tr>
<tr>
<td>AT88CK101STK8</td>
<td>Single-socket secure authentication development kit for Atmel ATAES132</td>
<td>PC</td>
<td>8-lead SOIC</td>
<td>Yes</td>
<td>Now</td>
</tr>
<tr>
<td>AT88CK109STK8</td>
<td>Dual-socket secure authentication development kit for Atmel ATAES132</td>
<td>PC</td>
<td>8-lead SOIC</td>
<td>Yes</td>
<td>Now</td>
</tr>
<tr>
<td>ATVRSERcurityX</td>
<td>Atmel ATAES132 security add-on board for Atmel AVR Xplained series</td>
<td>PC</td>
<td>8-lead SOIC</td>
<td>Yes</td>
<td>Now</td>
</tr>
</tbody>
</table>

For more information on the Atmel ATAES132, visit [http://www.atmel.com/MEM_ATSHA204](http://www.atmel.com/MEM_ATSHA204)

### Description

Atmel's CryptoAuthentication™ family of hardware security solutions has simplified the process of integrating security into embedded systems. The ATAES132, in particular, offers multiple evaluation and development support tools to meet the most aggressive development timelines. The very low-cost AT88CK427GREEN demonstration kit is a great starting point for designing secure systems. For more comprehensive evaluation and development capabilities, designers can choose from client or client and host kit configurations that include USB connectivity. This modular approach enables rapid and easy development in most development environments. Additionally, the ATVRSERcurityX Security Xplained add-on board 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](http://www.atmel.com).

---

**Disclaimer:** The information in this document is provided for general reference and may not be complete or up-to-date. It is not intended as a substitute for professional advice and the reader should verify the accuracy of the information before making any decisions. Atmel Corporation assumes no liability whatsoever and disclaims any express, implied, or statutory warranty relating to its products, including, but not limited to, the implied warranties 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 of 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.