



CryptoAuthentication Family of Crypto Elements with Hardware-Based Key Storage

ATSHA204A, ATAES132A and ATECC508A



CryptoAuthentication Devices Keep it Real

Atmel CryptoAuthentication™ crypto element devices with hardware-based key storage prevent would-be attackers from cloning, counterfeiting, or tampering with a product, the consumables it uses, the firmware it runs, the accessories that support it, and the network nodes to which it connects. Keeping products real helps maintain an OEM revenue flow by ensuring that only legitimate products can work in the host system and that would-be hackers cannot use them beyond their expiration date. Atmel offers the industry's widest selection of authentication devices featuring hardware-based key storage and cryptographic countermeasures that can evade even the most aggressive attacks. Attackers cannot attack because they cannot see the secret keys stored in protected hardware.

CryptoAuthentication Devices Make It Easy

CryptoAuthentication devices support modern cryptographic standards. They work with any microcontroller, are cost-effective, require only one GPIO, and use little power. Additionally, they operate over a wide voltage range and come in small packages. They feature built-in advanced protocols, including ECDSA (elliptic-curve digital-signature-algorithm) sign-verify capability for asymmetric authentication and ECDH elliptic-curve Diffie-Hellman, which provides key agreement in encryption/decryption settings. These features ease the addition of sophisticated security.

Cryptography involves many standards, algorithms, processes, definitions, and methods, and, as such, it is mathematically complex and highly detailed. Atmel does the more difficult cryptographic engineering, so users need not be crypto experts and can easily add robust security to digital systems.

CryptoAuthentication Uses

- Secure download and boot, ensuring in-transit authentication and protection of code
- Ecosystem control, ensuring that only authorized OEM and licensed nodes can access the hardware
- Anticlone, preventing identical BOM and stolen codes
- Message security, which ensures authentication, data integrity, and confidentiality of the network/IoT node





CryptoAuthentication Family of Crypto Elements with Hardware-Based Key Storage

ATSHA204A, ATAES132A and ATECC508A

CryptoAuthentication Key Features

	ATSHA204A	ATECC508A	ATAES132A
Description	Secure symmetric authentication crypto element device	High speed secure Elliptic Curve Cryptography (ECC) PKI asymmetric crypto element devices. (Backward compatibility with ATSHA204A.)	High-security, serial EEPROM providing authentication and confidential nonvolatile data storage.
Maximum Secure Count	1Kb	2 M for each of 2 counters	2M x 16
Function	Authentication	Authentication and FIPS SP800-56A ECDH key exchange for confidentiality and data integrity	Encryption/Authentication
Packages	UDFN8, SOIC8, SOT23-3, 3-Contact (RBH)	UDFN8, SOIC8, three-contact (RBH)	UDFN8, SOIC8
Authentication	SHA, HMAC (symmetric)	SHA, HMAC (symmetric), ECC (asymmetric)	AES-CCM (mutual, symmetric)
Crypto Algorithms	SHA256	SHA256, ECC-P256	AES128
Key Length	256	SHA=256; ECC=P256	128
I/O Interface	Single-wire I ² C	High-speed SPI with one GPIO Pin, 1MHz I ² C	I ² C, SPI
EEPROM Size	4.5Kb	10 Kb	32Kb (User), 2Kb (Keys)
Sleep	<150nA	<150nA	<250nA
Maximum Power	3mA	16mA	26mA
Vcc	2 to 5.5V	2 to 5.5V	2.5 to 5.5V
Key Offload and Reload			Yes
Factory-Unique ID	72 bits	72 bits	128 bits
Encrypted Read/Write	SHA / XOR	SHA / XOR	AES-CCM
Targets	Cost-sensitive applications, and those in which all components come from one OEM	Asymmetric applications, complex ecosystems, IoT	Drop-in replacements for serial EEPROM, systems that need to secure as much as 4Kb of data

Ordering information on Atmel web site.



Atmel Corporation 1600 Technology Drive, San Jose, CA 95110 USA **T:** (+1)(408) 441.0311 **F:** (+1)(408) 436.4200 | **www.atmel.com**

© 2015 Atmel Corporation. / Rev.: Atmel-8756F-ATSHA204A-ATEAS132-ATECC508A_E_US_112015

Atmel® Atmel logo and combinations thereof, Enabling Unlimited Possibilities®, and others are registered trademarks or trademarks of Atmel Corporation in U.S. and other countries. Other terms and product names may be trademarks of others.

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.