# 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
- Anticloning, 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 I²C | High-speed SPI with one GPIO Pin, 1MHz I²C | I²C, 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 | Enabling Unlimited Possibilities®

**Atmel Corporation** 1600 Technology Drive, San Jose, CA 95110 USA **T :** (+1)(408) 441. 0311 **F :** (+1)(408) 436. 4200 | **www.atmel.com**