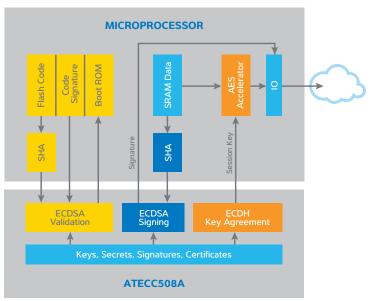


CryptoAuthentication[™] ATECC508A Crypto Element with ECDH and ECDSA



The Atmel[®] ATECC508A Crypto Element device with hardware-based key storage supports ECDH (ellipticcurve Diffie-Hellman) operation to provide key-agreement function. The ATECC508A is the second device with advanced elliptic-curve (ECC) capabilities in the Atmel CryptoAuthentication[™] portfolio.



Target Applications

This device is ideal for emerging Internet of Things (IoT) and traditional applications because ECDH key agreement enables confidentiality when users employ it with microprocessors running encryption/decryption algorithms, such as AES (Advanced Encryption Standard). Built-in ECDH eases key agreement and increases security between network nodes and host/ client applications. This Crypto Element addresses market segments such as home automation, industrial networking, accessory and consumable authentication, medical, mobile, and others. Users can employ the device with any microprocessor. It features extremely low power consumption and a wide voltage range. It requires only one GPIO (general-purpose input/output) pin and comes in tiny packages. A range of evaluation and development boards, software environments, code examples, and other materials support easy design-in.

Atmel

CryptoAuthentication[™] ATECC508A Crypto Element with ECDH and ECDSA

Key Features

- Optimized key storage and authentication
- ECDH operation using stored private key
- ECC-key generation
- ECDSA (elliptic-curve digital signature algorithm) Sign-Verify
- Support for X.509 certificate formats
- 256-bit SHA/HMAC (secure hash algorithm/ hash-based message authentication code) hardware engine
- Multilevel RNG (random number generator) using FIPS (Federal Information Processing Standard) SP 800–90A DRBG (deterministic random-bit generator)
- Guaranteed 72-bit unique ID
- · I2C and single-wire interfaces
- 2 to 5.5V operation, 150-nA standby current
- 10.5-kbit EEPROM for secret and private keys
- · Configuration ability for secret and private keys or data
- Ability for eight slots to store public keys, signatures, or certificates
- High Endurance Monotonic Counters
- UDFN, SOIC, and 3-lead contact packages

Part Number	Description
ATECC508A-SSHCZ	Crypto Element with ECDH and ECDSA, Single-Wire Interface in 8-lead SOIC
ATECC508A-SSHDA	Crypto Element with ECDH and ECDSA, I2C Interface in 8-lead SOIC
ATECC508A-MAHCZ	Crypto Element with ECDH and ECDSA, Single-Wire Interface in 8-pad UDFN
ATECC508A-MAHDA	Crypto Element with ECDH and ECDSA, I2C Interface in 8-pad UDFN
ATECC508A-RBHCZ	Crypto Element with ECDH and ECDSA, Single-Wire Interface in 3-lead Contact Package



F: (+1)(408) 436. 4200

Atmel Enabling Unlimited Possibilities[®]



Atmel Corporation

1600 Technology Drive, San Jose, CA 95110 USA

T: (+1)(408) 441.0311

www.atmel.com

© 2015 Atmel Corporation. / Rev.: Atmel-8938A-Crypto-ATECC508A-Flyer_E_US_022015

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 LABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RE-LATINGS TO ITS PRODUCTS INCLUDING, BUT NOT LIVITED TO THE INTERVISION OF MERCHAINTABILITY, ITTNESS FOR A PARTICULAR PURPOSE, OR NON-INFIRINGEMENT, IN NO EVENT SHALL ATMEL BE LED OR STATUTORY WARRANTY RE-LATINGS TO ITS PRODUCTS INCLUDING, BUT NOT LIVITED TO THE INTERVISION OF MERCHAINTABILITY, ITTNESS FOR A PARTICULAR PURPOSE, OR NON-INFIRINGEMENT, IN NO EVENT SHALL ATMEL BE LED OR STATUTORY WARRANTY TO USE THIS DOCUMENT, EVEN IF ATTNEL HAS BEEN ADMSED OF THE DSSIBILITY OF SUCH DAMAGES FOR LOSS AND PROFITS, BUSINESS INTERRUPTION, OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ATTNEL HAS BEEN ADMSED 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 are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.

X-ON Electronics

Largest Supplier of Electrical and Electronic Components

Click to view similar products for Security/Authentication Development Tools category:

Click to view products by Microchip manufacturer:

Other Similar products are found below :

MAXREFDES132# IPL-003WR AT88CK460WHITE ATCRYPTOAUTH-XPRO BLOCKCHAINSTARTKITTOBO1 DS28C40EVKIT# MAXREFDES143# AT88CK590 AT88CKECC-AWS-XSTK-B ATCRYPTOAUTH-XPRO-B DM320109 DM320118 DT100104 MIKROE-3746 MIKROE-3774 MIKROE-3915 MIKROE-4236 MIKROE-1819 MIKROE-2829 MIKROE-3045 OM-SE050ARD 102010288 AT97SC3205P-SDK2 MAXREFDES34# AT88CKECC-AWS-XSTK MIKROE-2761 MAXREFDES155# MIKROE-2760 MIKROE-2522 MIKROE-2733 cs-pastilda-01 CS-SOMU-02 103030395