AVAQ

ATECC508A-SSHDA-B

Authenticator CMOS 10KB 8-Pin SOIC N Tube

Manufacturer:	Microchip Technology, Inc
Package/Case:	SOP8
Product Type:	Embedded Processors & Controllers
RoHS:	RoHS Compliant/Lead free RoHS
Lifecycle:	NRND

ATECC508A-SSHDA-B Image

Images are for reference only

Inquiry

General Description

The ATECC508A crypto element is the first crypto device to integrate ECDH (Elliptic Curve Diffie–Hellman) key agreement, which makes it easy to add confidentiality (encryption/decryption) to digital systems including Internet of Things (IoT) nodes used in home automation, industrial networking, accessory and consumable authentication, medical, mobile and other applications. In addition to ECDH, the ATECC508A has ECDSA sign-verify capabilities built-in to provide highly secure asymmetric authentication. The combination of ECDH and ECDSA makes the device an ideal way to provide all three pillars of security such as confidentiality, data integrity, and authentication when used with MCU or MPUs running encryption/decryption algorithms (i.e. AES) in software. Similar to all Microchip CryptoAuthentication products, the new ATECC508A employs ultra-secure hardware-based cryptographic key storage and cryptographic countermeasures which are more secure than software-based key storage. This next-generation CryptoAuthentication device is compatible with any microprocessor (MPU) or microcontroller (MCU) including SMART and Microchip AVR MCUs or MPUs. As with all CryptoAuthentication devices, the ATECCC508A delivers extremely low-power consumption, requires only a single GPIO over a wide voltage range, and has a tiny form factor making it ideal for a variety of applications including those that require longer battery life and flexible form factors. The ATECC508A is downward compatible with the ATECC108A, ATECC108, ATSHA204A, and ATSHA204 crypto element devices.

The Microchip ATECC508A integrates ECDH (Elliptic Curve Diffie Hellman) security protocol an ultra-secure method to provide key agreement for encryption/decryption, along with ECDSA (Elliptic Curve Digital Signature Algorithm) sign-verify authentication for the Internet of Things (IoT) market including home automation, industrial networking, accessory and consumable authentication, medical, mobile and more.The ATECC508A is a secure element from the Microchip CryptoAuthentication portfolio with advanced Elliptic Curve Cryptography (ECC) capabilities. With ECDH and ECDSA being built right in, this device is ideal for the rapidly growing IoT market by easily supplying the full range of security such as confidentiality, data integrity, and authentication to systems with MCU or MPUs running encryption/decryption algorithms (i.e. AES).Similar to all Microchip CryptoAuthentication products, the new ATECC508A employs ultra-secure hardware-based cryptographic key storage and cryptographic countermeasures which are more robust than software-based key storage.The device is compatible with any microprocessor (MPU) or microcontroller (MCU) including Microchipand Microchip AVR/ARM MCUs or MPUs.As with all CryptoAuthentication devices, the ATECCC508A delivers extremely low-power consumption, requires only a single GPIO over a wide voltage range, and has a tiny form factor making it ideal for a variety of applications that require longer battery life and flexible form factors.

Key Features

Easy way to run ECDSA and ECDH Key Agreement

ECDH key agreement makes encryption/decryption easy

Ideal for IoT node security

Authentication without the need for secure storage in the host

No requirement for high-speed computing in client devices

Cryptographic accelerator with Secure Hardware-based Key Storage

Performs High-Speed Public Key (PKI) Algorithms

NIST Standard P256 Elliptic Curve Support

SHA-256 Hash Algorithm with HMAC Option

Host and Client Operations

256-bit Key Length

Storage for up to 16 Keys

Two high-endurance monotonic counters

Guaranteed Unique 72-bit Serial Number

Internal High-quality FIPS Random Number Generator (RNG)

10Kb EEPROM Memory for Keys, Certificates, and Data

Storage for up to 16 Keys

Multiple Options for Consumption Logging and One Time Write Information

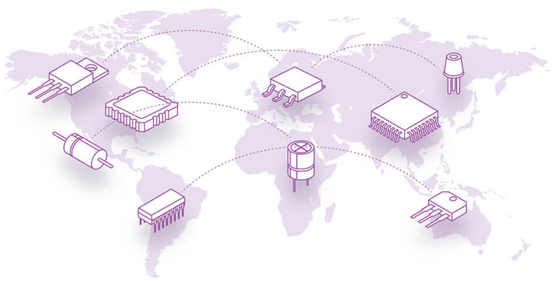
Intrusion Latch for External Tamper Switch or Power-on Chip Enablement

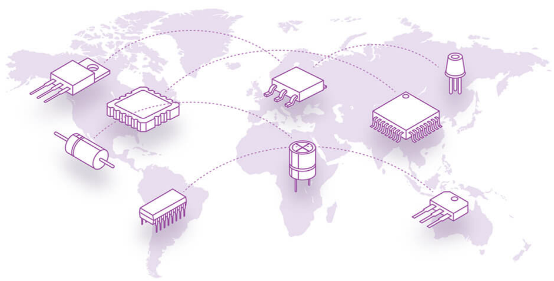
Single Wire or I2C Interface

2.0V to 5.5V Supply Voltage Range

1.8V to 5.5V IO levels

8-pad UDFN,8-lead SOIC, and 3-lead CONTACT Packages





AVAQ AVAQ

Recommended For You

ATECC508A-MAHDA-S	Microchip Technology, Inc	UDFN8
ATSHA204A-SSHDA-B	Microchip Technology, Inc	SOP8
ATECC608B-SSHDA-B	Microchip Technology, Inc	SOP8
ATECC608A-MAHDA-S	Microchip Technology, Inc	UDFN8
ATECC608A-SSHDA-B	Microchip Technology, Inc	SOP8
ATECC608A-SSHDA-T	Microchip Technology, Inc	SOP-8
ATECC608A-MAHDA-T	Microchip Technology, Inc	UDFN8
ATSHA204-SH-DA-T	Microchip Technology, Inc	SOP-8
ATECC608B-MAHDA-S	Microchip Technology, Inc	UDFN8
ATECC508A-SSHDA-T	Microchip Technology, Inc	SOP8
ATSHA204A-MAHCZ-T	Microchip Technology, Inc	UDFN-8
ATECC608B-SSHDA-T	Microchip Technology, Inc	SOP8
ATECC608A-SSHCZ-T	Microchip Technology, Inc	SOIC-8
ATSHA204A-SSHCZ-T	Microchip Technology, Inc	SOIC-8
ATECC108A-MAHDA-T	Microchip Technology, Inc	UDFN-8