


Crypto-Authentication™ 8-Pin SOIC N Tube

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

Images are for reference only

[Inquiry](#)

General Description

The Microchip ATECC608A 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, medical, as well as accessories and consumables authentication and more. In addition, the ATECC608A offer an integrated AES hardware accelerator strengthening hardware based security for LoRaWAN applications and enable secure boot capabilities for very small microcontrollers. The ATECC608A 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. Similar to all Microchip CryptoAuthentication products, the new ATECC608A employs ultra-secure hardware-based cryptographic key storage and cryptographic countermeasures which eliminate potential backdoors linked to software weaknesses. The device is agnostic of any microprocessor (MPU) or microcontroller (MCU) and compatible with Microchip AVR/ARM MCUs or MPUs. As with all CryptoAuthentication devices, the ATECC608A 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.

Take a look at the various use cases including :

- Cloud authentication for AWS IoT (32-bit)
- Cloud Authentication for AWS IoT Greengrass (Linux)
- Cloud Authentication for Google Cloud IoT Core
- LoRa Authentication for The Things Industries (TTI)
- Secure Boot implementation with an ATSAM21 Cortex-M0+

Key Features

Protected storage for up to 16 Keys, certificates or data

Hardware support for asymmetric sign, verify, key agreement – ECDSA: FIPS186-3 Elliptic Curve Digital Signature

ECDH: FIPS SP800-56A Elliptic Curve Diffie-Hellman

NIST standard P256 elliptic curve support

Hardware support for symmetric algorithms

SHA-256 & HMAC hash including off-chip context save/restore

AES-128: encrypt/decrypt, galois field multiply for GCM

Networking key management support

Turnkey PRF/HKDF calculation for TLS 1.2 & 1.3

Ephemeral key generation and key agreement in SRAM – Small message encryption with keys entirely protected

Secure boot support

Full ECDSA code signature validation, optional stored digest/signature – optional communication key disablement prior to secure boot

Encryption/Authentication for messages to prevent on-board attacks

Internal high-quality FIPS 800-90 A/B/C Random Number Generator (RNG)

Two high-endurance monotonic counters

Guaranteed unique 72-bit serial number

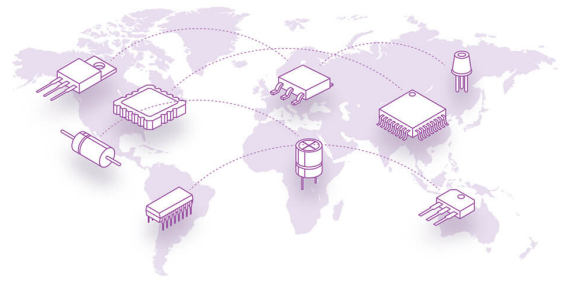
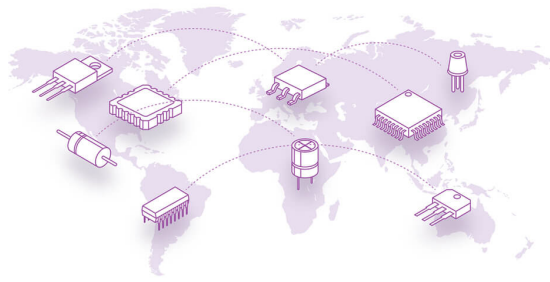
Two interface options available

High-speed single pin interface with One GPIO pin

1MHz Standard I2C interface

1.8V to 5.5V IO levels, 2.0V to 5.5V supply voltage

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



Recommended For You

ATECC508A-MAHDA-S

Microchip Technology, Inc

UDFN8

ATSHA204A-SSHDA-B

Microchip Technology, Inc

SOP8

ATECC608B-SSHDA-B

Microchip Technology, Inc

SOP8

ATECC508A-SSHDA-B

Microchip Technology, Inc

SOP8

ATECC608A-MAHDA-S

Microchip Technology, Inc

UDFN8

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