ATAES132A-MAHER-T

Data Sheet

32Kbit AES Authentication I2C UDFN, GR - 32Kbit AES Auth I2C udfn(MA), GR

Manufacturers	Microchip Technology, Inc
Package/Case	8-UFDFN
Product Type	Integrated Circuits (ICs)
RoHS	
Lifecycle	

Images are for reference only

Please submit RFQ for ATAES132A-MAHER-T or Email to us: sales@ovaga.com We will contact you in 12 hours. RFQ

General Description

Authorization, Key Management, and Memory Encryption

The first device in the AES family, the ATAES132A, is a high-speed, high-security, 32K Serial EEPROM that enables authentication and confidential nonvolatile data storage. It is a direct drop-in for industry standard Serial EEPROMS and is an easy way to add security to a system. The ATES132A includes a high-quality hardware Random Number Generator (RNG) paired with a Federal Information Processing Standards (FIPS) Deterministic Random Bit Generator (DRBG) to prevent replay attacks.This ATAES132A uses the industry standard Advanced Encryption Standard (AES) algorithm in the CCM mode (Counter and Cipher block chaining Message authentication code) making authentication, confidentiality, and data integrity checking easy.Data encryption and decryption can be easily performed for both internally stored data or for small external data packets (depending upon the configuration). Data encrypted by one AES device can be decrypted by another, and vice versa. The secure Serial EEPROM architecture of the ATAES132A and packages compatible with standard SPI and I2C EEPROM footprints allow direct insertion into many existing Serial EEPROM applications. A wide array of defense mechanisms are designed to prevent physical attacks on the device itself, as well as logical attacks on the data transmitted between the device and the system. All CryptoAuthentication devices, including the ATAES132A are equipped with secure personalization features to facilitate third-party product manufacturing.The ATAES132A crypto element with hardware-based key storage is a very fast high-security serial 32K EEPROM device that enables authentication and confidential nonvolatile data storage. It is a direct drop-in for industry standard Serial EEPROMS, and supports the Advanced Encryption Standard (AES) cryptography standard. The AES-128 cryptographic engine operates in AES-CCM mode to provide authentication, stored data encryption/decryption, and Message Authentication Codes (MACs). Data encryption/decryption can be performed for internally stored data or for small external data packets depending upon the configuration. Data encrypted by one ATAES132A device can be decrypted by another, and vice versa.Extended security functions are accessed by sending command packets to the ATAES132 using standard write instructions and reading responses using standard read instructions. The device incorporates multiple physical security mechanisms to prevent release of the internally stored secrets. The device's secure Serial EEPROM architecture and packages compatible with standard SPI and I2C EEPROM footprints allow insertion into many existing Serial EEPROM applications. Like all Microchip CryptoAuthentication devices the ATAES132A stores keys and other secret data in hardware protected by a range of physical and cryptographic countermeasures, making it far more secure than software or unprotected hardware storage mechanisms.

Features

32Kb Standard Serial EEPROM User Memory (16 User Zones of 2Kb)

AES Algorithm with 128-bit Keys

AES-CCM for Authentication

Secure Storage for 16 and 128 bit Keys

Encrypted User Memory Read and Write

FIPS Random Number Generator (RNG)

16 High-Endurance Monotonic EEPROM Counters

Authentication Prior to Zone Access

Read/Write, Encrypted, or Read-only User Zone Options

SPI and I2C Interface Options

2.5V to 5.5V Supply, <250nA Sleep

Serial EEPROM Compatible Pinout (SOIC, SOP, or UDFN)

Easily Add Security by Replacing Existing Serial EEPROM

Authenticate Consumables, Components, and Network Access

Protect Sensitive Firmware

Securely Store Sensitive Data and Enable Paid-for Features

Prevent Contract Manufacturers from Overbuilding

Manage Warranty Claims

Securely Store Identity Data (i.e. Fingerprints and Pictures)

Related Products

ATA6563-GAQW0

Microchip Technology, Inc

SOIC-8

AT42QT1040-MMHR

Microchip Technology, Inc

VQFN-20

AT30TSE004A-MAA5M-T

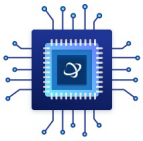
Microchip Technology, Inc

WDFN-8

AT30TS74-SS8M-T

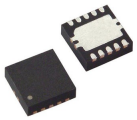
Microchip Technology, Inc

SOIC-8



ATMEGA808-MU

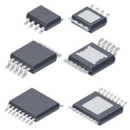
Microchip Technology, Inc



ATSAMC21G17A-MZTVAO

Microchip Technology, Inc

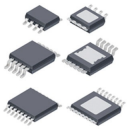
VQFN



ATTINY3226-SU

Microchip Technology, Inc

SOIC



ATTINY3224-SSU

Microchip Technology, Inc

SOIC