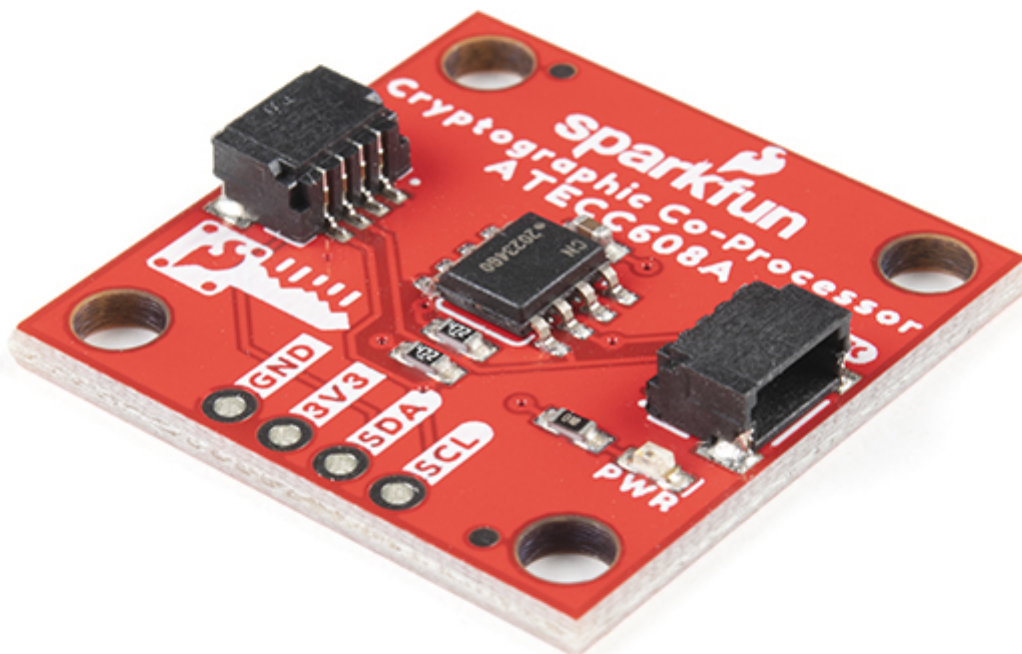# SparkFun Cryptographic Co-Processor Breakout - ATECC608A (Qwiic)

☐ **Product Restrictions:** To access certain features of the ATECC608A, users will need to contact Microchip and sign an NDA contract to obtain the complete datasheet. Due to the required NDA - technical support, an Arduino library, and hookup guide are not provided for users on this product.

The SparkFun ATECC608A Cryptographic Co-processor Breakout allows you to add strong security to your IoT node, edge device, or embedded system. This includes **asymmetric** authentication, **symmetric** AES-128 encryption/decryption, and much more. As stated above, the ATECC608A has limited Arduino support and the complete datasheet is under NDA with Microchip.

This breakout board includes two Qwiic ports for plug and play functionality. Utilizing our handy Qwiic system, no soldering is required to connect it to the rest of your system. However, we still have broken out 0.1"-spaced pins in case you prefer to use a breadboard. The ATECC608A chip is capable of many cryptographic processes, including, but not limited to:

- Creating and securely storing unique asymmetric key pairs based on Elliptic Curve Cryptography (FIPS186-3).
- AES-128: Encrypt/Decrypt, Galois Field Multiply for GCM
- Creating and verifying 64-byte digital signatures (from 32-bytes of message data).
- Creating a shared secret key on a public channel via Elliptic Curve Diffie-Hellman Algorithm.
- SHA-256 & HMAC Hash including off-chip context save/restore
- Internal high quality FIPS random number generator.

Embedded in the chip is a 10Kb EEPROM array that can be used for storing keys, certificates, data, consumption logging, and security configurations. Access to the sections of memory can then be restricted and the configuration locked to prevent changes. Each ATECC608A Breakout ships with a guaranteed unique 72-bit serial number and includes several security features to prevent physical attacks on the device itself, or logical attacks on the data transmitted between the device.

A summary datasheet for the ATECC608A is available here. The full datasheet is under NDA with Microchip. You will need to contact them for access to the entire datasheet. Meanwhile, the ArduinoATECCX08 Library currently only supports the ATECC608A with SAMD21 Arduino boards.

We do have much more support for the ATECC508A version of this chip. Please check out our ATECC508A Hookup Guide and Arduino Library (which includes six examples). This will get you familiar with the basics of elliptic curve cryptography and signing/verifying data with the ATECC508A version of the chip.

Note: The I²C address of the ATECC608A is 0x60 and is software-configurable to any address. A multiplexer/Mux is required to communicate to multiple ATECC608A sensors at the default address when on a single bus. If you need to use more than one ATECC608A sensor at the default address, consider using the Qwiic Mux Breakout. 🔒 **Note:** The ATECC608A can be only configured once before it is **PERMANENTLY** locked. It is advisable that users purchase multiple boards in order to use other configurations and explore the advanced functions of the ATECC608A.

Additionally, this board **IS** capable of encrypting and decrypting data. However, to access these additional features, you will need to contact Microchip and sign an NDA contract to obtain the complete datasheet.

It is recommended that an SparkFun RedBoard Turbo - SAMD21 Development Board is used with this product due to the buffer size required on the I²C bus.

The SparkFun Qwiic Connect System is an ecosystem of I²C sensors, actuators, shields and cables that make prototyping faster and less prone to error. All Qwiic-enabled boards use a common 1mm pitch, 4-pin JST connector. This reduces the amount of required PCB space, and polarized connections mean you can't hook it up wrong.