Datenblatt

SparkFun Qwiic - Kryptographischer Co-Prozessor Breakout, ATECC508A

Numero Ordine:	DEV-15573
Hersteller:	SparkFun
Herkunftsland:	USA
Zolltarifnummer:	84733020
Gewicht:	0.002 kg

Mit dem SparkFun ATECC508A Cryptographic Co-processor Breakout können Sie auf einfache Weise starke Authentifizierungssicherheit zu Ihrem IoT-Knoten, Edge Device oder Embedded System hinzufügen. Er enthält zwei Qwiic-Ports für Plug-and-Play-Funktionalität. Durch die Verwendung unseres praktischen Qwiic-Systems ist kein Löten erforderlich, um ihn mit dem Rest Ihres Systems zu verbinden. Dennoch haben wir die Pins im 0,1"-Abstand herausgebrochen, falls Sie lieber ein Breadboard verwenden möchten. Der ATECC508A-Chip ist in der Lage, viele kryptografische Verfahren durchzuführen, u.a.:

- Erzeugen und sicheres Speichern von eindeutigen asymmetrischen Schlüsselpaaren basierend auf Elliptic Curve Cryptography (FIPS186-3).
- Erstellen und Verifizieren von 64-Byte-Digitalsignaturen (aus 32-Byte-Nachrichtendaten).
- Erzeugen eines gemeinsamen geheimen Schlüssels auf einem öffentlichen Kanal über den Elliptic Curve Diffie-Hellman Algorithmus.
- Ein Standard-Hash-basiertes Challenge-Response-Protokoll unter Verwendung eines SHA-256-Algorithmus.
- Interner hochqualitativer FIPS-Zufallszahlengenerator.

Eingebettet in den Chip ist ein 10Kb EEPROM-Array, das für die Speicherung von Schlüsseln, Zertifikaten, Daten, Verbrauchsprotokollierung und Sicherheitskonfigurationen verwendet werden kann. Der Zugriff auf die Speicherbereiche kann dann eingeschränkt und die Konfiguration gesperrt werden, um Änderungen zu verhindern.

Jeder ATECC508A wird mit einer garantiert eindeutigen 72-Bit-Seriennummer ausgeliefert und enthält mehrere Sicherheitsfunktionen, um physische Angriffe auf das Gerät selbst oder logische Angriffe auf die zwischen dem Gerät übertragenen Daten zu verhindern.

Mit unserem Hookup-Guide und der Arduino-Library (mit sechs Beispielen) sind Sie im Handumdrehen mit den Grundlagen der elliptischen Kurven-Kryptografie und dem Signieren/Verifizieren von Daten vertraut!

 Hinweis: Bitte lesen Sie die Hookup-Anleitung vollständig durch, bevor Sie dieses Board verwenden. Der Chip kann nur konfiguriert werden, bevor er **PERMANENT** verriegelt wird. Es ist ratsam, dass Benutzer mehrere Boards kaufen, um andere Konfigurationen zu verwenden und die erweiterten Funktionen des ATECC508A zu erkunden.

Außerdem ist dieses Board **NICHT** in der Lage, Daten zu verschlüsseln und zu entschlüsseln. Es kann jedoch einige kryptografische

Authentifizierungsprozesse durchführen, wie z.B. die sichere Erstellung von privaten Schlüsseln, die sichere Speicherung von Schlüsseln und die Erstellung und Überprüfung von digitalen Signaturen.

Aufgrund der erforderlichen Puffergröße auf dem I2C-Bus wird empfohlen, ein Artemis-Mikrocontroller-Board mit diesem Produkt zu verwenden.

Features:

- Betriebsspannung: 2,0V-5,5V (**Standard bei Qwiic-System: 3,3V**)
- Aktive Stromaufnahme (für ATECC508A): 16 mA
- Sleep-Strom (für ATECC508A): <150 nA
- Garantiert eindeutige 72-Bit-Seriennummer
- 10 Kb EEPROM-Speicher für Schlüssel, Zertifikate und Daten
    - Speicherplatz für bis zu 16 Schlüssel
    - 256-Bit-Schlüssellänge
- Interner hochqualitativer FIPS-Zufallszahlengenerator (RNG)
- Konfigurierbare I2C-Adresse (7-Bit): 0x60 (**Default**)

Dokumente:

- Get Started with the Cryptographic Co-processor Breakout Guide
- Schaltplan
- Eagle-Dateien
- Platinenabmessungen
- Anschlussanleitung
- Datenblatt (ATECC508A)
- SparkFun ATECCX08A Arduino Library
- Github Hardware Repo

Weitere Bilder: