In der heutigen enorm IoT-vernetzten Welt wird das Kriterium Sicherheit innerhalb eines Kundenprodukts oder -systems immer mehr zu einer unerlässlichen Anforderung. Von einer Anwendung zur anderen können die Sicherheitsanforderungen drastisch variieren: Verhinderung von unbefugtem Zutritt oder Zugriff, von Diebstahl geistigen Eigentums an Software/Hardware, von Daten oder von Kommunikationsdienstleistungen. Eine solche Anwendung ist ein Zutrittskontollsystem in Gebäuden.Microchip vereint sowohl kryptographische und nicht-kryptographische Komponenten, um eine Komplettlösung zu erstellen. Sicherheit bedeutet heutzutage vor allem Vertrauen. Sicherheitsprodukte von Microchip machen es einfach, "Vertrauen" in jedes System zu integrieren. Aufgrund ihrer Flexibilität, erweiterten Funktionen, innovativen und kostengünstigen Architekturen und extrem sicheren Hardware-Schutzmechanismen sind die auf Microchip Hardware basierenden Sicherheitssysteme der ideale Weg, Vertrauen schon beim Design zu integrieren.

Board	**Link**
Atmel ATSHA204A	https://www.digikey.at/de/product-highlight/a/atmel/atsha204a-full-turnkey-security-device
Symmetric Key storage and Cryptographic Coprocessor	
Security Features: Der ATSHA204A von Microchip ist komplett schlüsselfertig. Er enthält ein in sechzehn Slots aufgeteiltes 4,5-kB-EEPROM. Dieses Array kann für die Speicherung von Schlüsseln, verschiedene Lese-/Schreibvorgänge, Nur-Lesevorgänge, Passwörter oder geheime Daten und zur Verbrauchserfassung verwendet werden. Der Zugriff auf die verschiedenen Speicherabschnitte kann auf verschiedene Weise eingeschränkt werden und dann kann die Konfiguration gesperrt werden, um Änderungen zu verhindern - Krypto-Element mit geschütztem, Hardware-basiertem Schlüsselspeicher - Sichere, symmetrische Host- und Client-Operationen des Authentifizierungs-Geräts - Der überlegene SHA-256 verfügt über einen Hash-Algorithmus mit Message-Authentication-Code (MAC) und Hash-basierten Message-Authentication-Code(MAC)-Optionen. - Marktführende 256 Bit Schlüssellänge; Speicher für bis zu 16 Tasten - Garantierte, einzigartige, 72-Bit-Seriennummer - Interner, qualitativ hochwertiger Zufallszahlengenerator (RNG)	

Board	Link
Atmel ATECC508A	https://www.digikey.at/de/product-highlight/a/atmel/atsha204a-full-turnkey-security-device

Symmetric/Assymetric Key storage and Cryptographic Coprocessor

Security Features:

Die Microchips-Komponente ECC508A bietet ZeroTouch für die AWS-IoT-Secure-Provisioning-Plattform für AWS-IoT und bietet damit die branchenweit erste durchgehende Sicherheitslösung für Internet-der-Dinge(IoT)-Komponenten, die sich mit Amazon Web Services (AWS) verbinden. Das Produkt wurde gemeinsam mit AWS entwickelt und unterstützt IoT-Geräte bei der schnellen und einfachen Compliance mit dem AWS-IoT-Sicherheitsmodell der gegenseitigen Authentifizierung. Das neue Sicherheitsmodell besagt, dass eine Komponente gegenseitige Authentifizierung mit einem Remote-Server nutzen muss, um für die AWS-Cloud autorisiert zu werden.

- Nahtlose Integration des AWS IoT in jedes IoT-Produkt
- So einfach, wie eine vorgefertigte ECC508-Komponente auf die Platine zu löten
- Gemeinsam mit AWS entwickelt, um Einhaltung der AWS-IoT-Sicherheitsrichtlinien zu gewährleisten
- Nach erstmaliger Verbindung automatisches Selbsteinloggen in AWS-Servern ohne Nutzerintervention
- Manipulationssicheres Secure Element für eine sichere Authentifizierung durch Schlüsselspeicher und sichere Ausführungsumgebungen
- Für immer geheime, intern generierte private Geräteschlüssel zur Erleichterung der Fertigungs-Logistik und des Chain-of-Trust-Managements
- Flexible Optionen für Gehäuse und Schnittstellenkommunikation
- Schlüssel-Bereitstellung für Großserienfertigung leicht gemacht
- Verschiedene Optionen, um eine Vertrauenskette (chain of trust) mit einem selbst signierten Root- oder einem allgemein anerkannten Autorisierungs-Zertifikat einzurichten

Board	Link
Atmel ATECC608A	https://www.ineltek.com/protect-ip-and-deploy-secured-connected-systems-with-microchips-new-cryptoauthentication-device-and-security-design-partner-program/ https://www.digikey.at/de/articles/techzone/2018/jun/use-a-crypto-chip-to-add-secure-boot-to-iot-device-designs

Symmetric/Assymetric Key storage and Cryptographic Coprocessor with enhancements for secure boot and secure connectivity

Security Features:

From remote cyber-attacks to the creation of counterfeit products, security threats are wide-spread and affect all industries. When carried out, these threats can translate into substantial losses in service revenue, recovery costs and, perhaps most significantly, in brand equity. Implementing robust security into new and existing designs to protect Intellectual Property (IP) and enable trusted authentication of connected devices is critical. To protect against these threats, Microchip Technology Inc. has created the ATECC608A CryptoAuthentication™ device, a secure element that allows developers to add hardware-based security to their designs. Microchip has also established a Security Design Partner Program for connecting developers with third-party partners that can enhance and expedite secure designs.

The foundation of secured communication is the ability to create, protect and authenticate a device's unique and trusted identity. By keeping a device's private keys isolated from the system in a secured area, coupled with its industry-leading cryptography practices, the ATECC608A provides a high level of security that can be used in nearly any type of design. Primary features of the ATECC608A include:

- Best-in-class key generation:
  The Federal Information Processing Standard (FIPS)-compliant Random Number Generator (RNG) generates unique keys that comply with the latest requirements from the National Institute of Standards and Technology (NIST), providing an easier path to a whole-system FIPS certification.
- Boot validation capabilities for small systems:
  New commands facilitate the signature validation and digest computation of the host microcontroller (MCU) firmware for systems with small MCUs, such as an ARM® Cortex®-M0+ based device, as well as for more robust embedded systems.
- Trusted authentication for LoRa nodes:
  The AES-128 engine also makes security deployments for LoRa infrastructures possible by enabling authentication of trusted nodes within a network.
- Fast cryptography processing:
  The hardware-based integrated Elliptical Curve Cryptography (ECC) algorithms create smaller keys and establish a certificate-based root of trust more quickly and securely than other implementation approaches that rely on legacy methods.
- Tamper-resistant protections:
  Anti-tampering techniques protect keys from physical attacks and attempted intrusions after deployment. These techniques allow the system to preserve a secured and trusted identity.
- Trusted in-manufacturing provisioning:
  Companies can use Microchip's secured manufacturing facilities to safely provision their keys and certificates, eliminating the risk of exposure during manufacturing.

Board	Link
Atmel ATAES132A	https://www.channel-e.de/nachrichten/article/eeprom-with-aes-ccm-authentication.html

32 Kb High Security Serial EEPROM Memory with AES-128 Cryptographic AES-CCM engine

Security Features:

These devices offer secure data storage using the AES (Advanced Encryption Standard) authentication for industrial, consumer, computing and embedded applications with flexible key management features and secure counters. AES is a symmetric-key encryption standard adopted by governments and cryptographic experts around the world.

These security features are available in two devices compatible with standard serial EEPROMs, one supporting I2C and the other supporting SPI. This allows system developers to add security to existing systems without retooling their printed circuit board. This direct replacement can extend the life of a system's architecture by including security features within the hardware to make the system more secure than software implementations.

The new secure devices also extend a current system's security into the future with the AES-CCM (AES in Counter and Cipher block chaining modes with message authentication code) authentication. The Atmel ATAES132 development kits can be plugged into a variety of Atmel AVR or ARM-based development kit for a complete project solution. All Atmel ATAES132 devices support 2.5V to 5.5V supply voltages and consume less than 250nA standby/sleep current.

MICROCHIP | ATECC608A CryptoAuthentication™ Device