Da heutzutage die Welt extrem IoT vernetzt ist, wird die Sicherheit in Kundenprodukten und -systemen immer wichtiger. Die Sicherheitsanforderungen können jedoch von Anwendung zu Anwendung sehr variieren. Das kann von der Verhinderung von unbefugtem Zutritt oder Zugriff über Diebstahl geistigen Eigentums an Software oder Hardware bis hin zu Diebstahl von Daten oder Kommunikationsdienstleistungen reichen. Sicherheit bedeutet in der heutigen Zeit vor allem Vertrauen.

Board	**Link**
Atmel ATSHA204A	https://www.digikey.at/de/product-highlight/a/atmel/atsha204a-full-turnkey-security-device
Symmetrische Schlüsselspeicherung und kryptografische Coprozessoren	

Security Features:

- komplett schlüsselfertig
- in 16 Slots aufgeteiltes 4,5-kB-EEPROM -> Verwendung: zur Speicherung von Schlüsseln, Lese-/Schreibvorgängen, Nur-Lesevorgängen, Passwörtern oder geheimen Daten und zur Verbrauchserfassung
- Zugriff auf verschiedene Speicherabschnitte auf unterschiedliche Art und Weise einschränken und anschließend besteht die Möglichkeit die Konfiguration zu sperren um Änderungen zu verhindern
- geschützter, Hardware-basierter Schlüsselspeicher
- Authentifizierungs-Gerät ist mit sicheren, symmetrischen Host-/Client-Operationen ausgestattet
- SHA-256 wird verwendet -> verfügt über: Hash-Algorithmus mit Message-Authentication-Code (MAC) und hashbasierten MAC-Optionen
- Schlüssellänge: 256 Bit -> Speicher für bis zu 16 Tasten
- 72-Bit-Seriennummer -> garantiert einzigartig
- RNG -> interner, qualitativ hochwertiger Zufallszahlengenerator

Board	**Link**
Atmel ATECC508A	https://www.digikey.at/de/product-highlight/a/atmel/atsha204a-full-turnkey-security-device
Symmetrische/Asymmetrische Schlüsselspeicherung und kryptografische Coprozessoren	

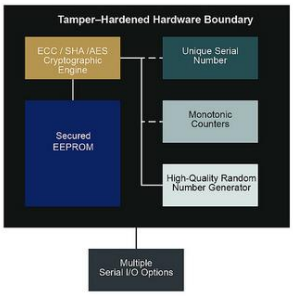
Security Features:

AWS – Amazon Web Services
IoT – Internet of Things

- ZeroTouch für AWS-IoT-Provisioning-Plattform für AWS-IoT
- Branchenweit erste durchgehende Sicherheitslösung für IoT-Komponenten welche sich mit AWS verbinden können.
- Gegenseitige Authentifizierung mit Remote-Servern zur Nutzung der AWS-Cloud
- Integration des AWS-IoT in andere IoT-Produkte sehr einfach
- Automatisches Selbsteinloggen nach erstmaliger Verbindung
- Sichere Authentifizierung wird gewährleistet durch Schlüsselspeicher und sichere Ausführungsumgebungen
- Zur Erleichterung der Fertigungs-Logistik und des Chain-of-Trust-Managements gibt es geheime, intern generierte private Geräteschlüssel
- Gehäuse und Schnittstellenkommunikation ist flexibel
- Erleichterung der Schlüssel-Bereitstellung für Großserienfertigungen
- Chain-of-Trust kann mit einem selbst signierten Root- oder einem allgemein anerkannten Autorisierungs-Zertifikat eingerichtet werden

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
Symmetrische/Asymmetrische Schlüsselspeicherung und kryptografische Coprozessoren mit Verbesserungen des Secure Boots und der sicheren Verbindung	
Security Features: • Erlaubt Hardware-basierte Sicherheit in ein Design einzufügen • RNG (Random Number Generator) generiert einzigartige Schüssel um das Gegenüber bei einer Unterhaltung authentifizieren zu können. • Boot Validierungsfähigkeiten für kleine Systeme (Embedded Systems) • Ermöglicht die Authentifizierung von vertrauenswürdigen Nodes in einem Netzwerk -> LoRA Nodes • Schnelle kryptografische Verarbeitung: die Hardware-basierten integrierten Elliptical Curve Cryptography (ECC) Algorithmen generieren kleinere Schlüssel, wodurch ein Zertifikat-basiertes Root of Trust schneller und sicher hergestellt werden kann. • Manipulations-resistent -> die Schlüssel werden von physikalischen Attacken sowie von versuchten Eingriffen nach der Entwicklung geschützt, was es dem System erlaubt die sichere und vertrauenswürdige Identität zu bewahren. • Unternehmen haben die Möglichkeit Microchip's sichere Fabriken zu verwenden um ihre Schlüssel und Zertifikate sicher bereitzustellen, ohne dem Risiko das bei der Herstellung eine Bloßlegung der vorher genannten Komponenten besteht.	

MICROCHIP ATECC608A CryptoAuthentication™ Device



Board	Link
Atmel ATAES132A	https://www.channel-e.de/nachrichten/article/eeprom-with-aes-ccm-authentication.html
32 kB serieller Hochsicherheits-EEPROM Speicher mit AES-128 kryptografischem AES-CCM Antrieb	
Security Features: • Sichere Datenspeicherung durch Advanced Encryption Standard (AES) Authentifizierung mit flexiblen Schlüsselmanagement Eigenschaften und sicheren Zählern. • Symmetrischer Schlüssel Verschlüsselungsstandard • AES-CCM Authentifizierung -> AES im Verkettungsmodus für Chiffrierblöcke und Counter Mode mit MAC	