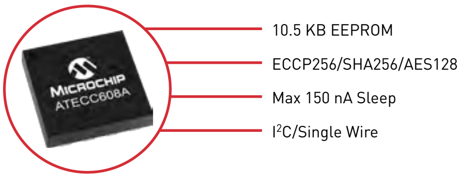
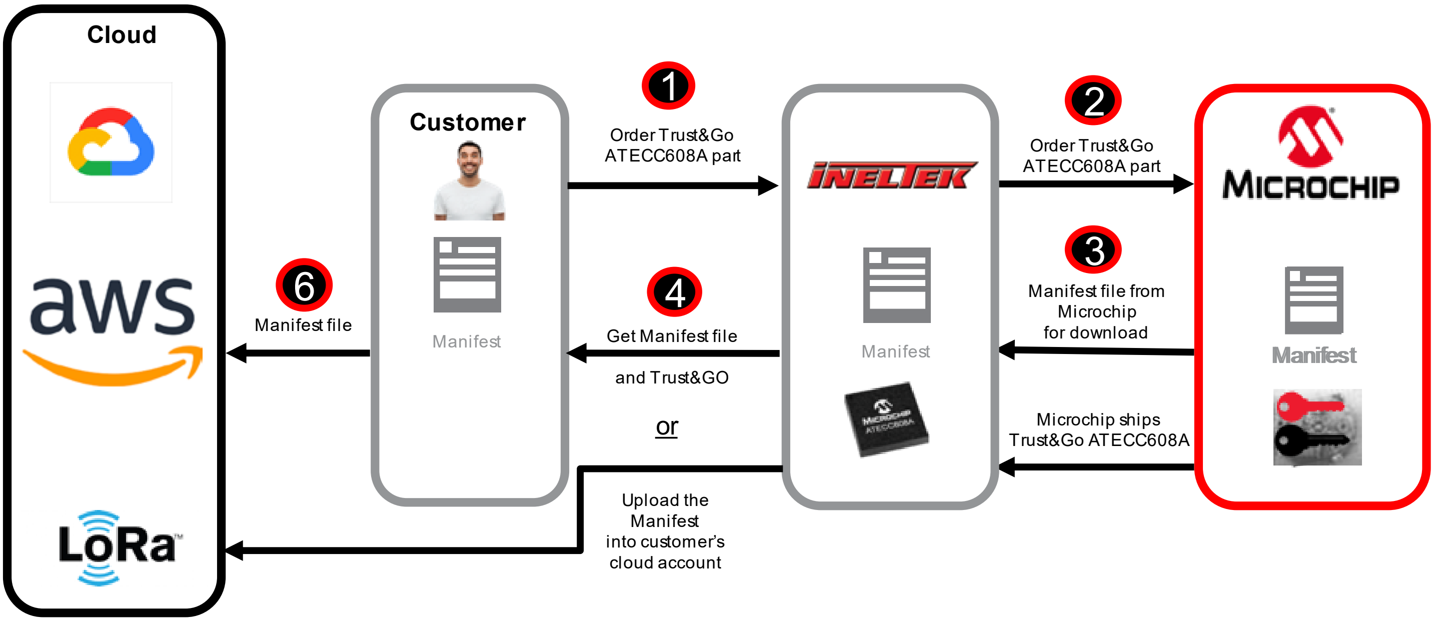
# Secure Elements and CryptoAuthentication

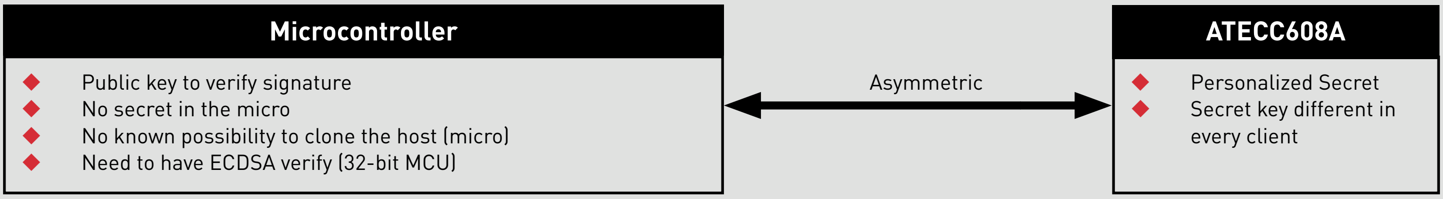
The Microchip ATECC608A is a secure element, part of the Trust Platform for the CryptoAuthentication family. The device integrates ECDH (Elliptic Curve Diffie Hellman) security protocol, an ultra-secure method to provide key agreement for encryption/decryption, along with ECDSA (Elliptic Curve Digital Signature Algorithm) sign-verify authentication. In addition, the ATECC608A offer an integrated AES hardware accelerator strengthening hardware-based security for cloud connectivity applications and enable secure boot capabilities for very small microcontrollers.



- Cryptographic co-processor with secure hardware-based key storage
- Protected storage for up to 16 Keys, certificates or data
- Hardware support for asymmetric sign, verify, key agreement – ECDSA: FIPS186-3 Elliptic Curve Digital Signature
- ECDH: FIPS SP800-56A Elliptic Curve Diffie-Hellman
- NIST standard P256 elliptic curve support
- Hardware support for symmetric algorithms
- SHA-256 & HMAC hash including off-chip context save/restore
- AES-128: encrypt/decrypt, galois field multiply for GCM
- Networking key management support
- Turnkey PRF/HKDF calculation for TLS 1.2 & 1.3
- Ephemeral key generation and key agreement in SRAM – Small message encryption with keys entirely protected
- Secure boot support
- Full ECDSA code signature validation, optional stored digest/signature – optional communication key disablement prior to secure boot
- Encryption/Authentication for messages to prevent on-board attacks
- Internal high-quality FIPS 800-90 A/B/C Random Number Generator (RNG)
- Guaranteed unique 72-bit serial number
- UDFN8 and SOIC8 Package options


Cloud
aws
LoRa
Customer
Manifest
INELTEK
Manifest
MICROCHIP
Manifest
1
Order Trust&Go ATECC608A part
2
Order Trust&Go ATECC608A part
3
Manifest file from Microchip for download
Microchip ships Trust&Go ATECC608A
4
Get Manifest file and Trust&GO
or
Upload the Manifest into customer's cloud account
6
Manifest file

# Secure Elements and CryptoAuthentication



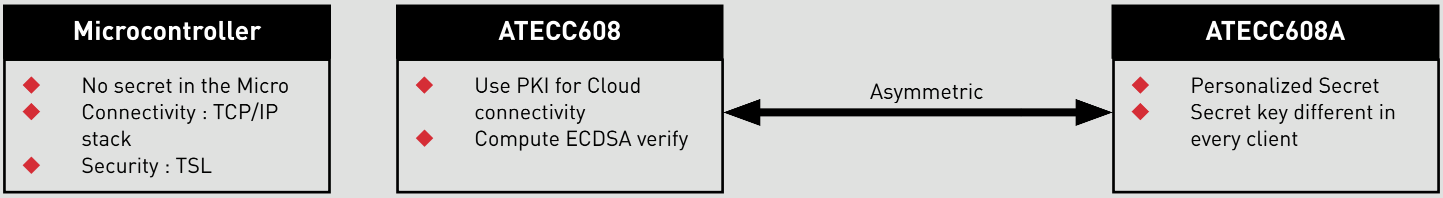
**Microcontroller**

- Public key to verify signature
- No secret in the micro
- No known possibility to clone the host (micro)
- Need to have ECDSA verify (32-bit MCU)

Asymmetric

**ATECC608A**

- Personalized Secret
- Secret key different in every client



**Microcontroller**

- No secret in the Micro
- Connectivity : TCP/IP stack
- Security : TSL

**ATECC608**

- Use PKI for Cloud connectivity
- Compute ECDSA verify

Asymmetric

**ATECC608A**

- Personalized Secret
- Secret key different in every client

## Trust Platform for the CryptoAuthentication™ Family

Are you looking for a quick and easy way to implement secure authentication for your Internet of Things (IoT) design? With the Trust&GO platform is designed to streamline the process of enabling network authentication using our ATECC608A secure elements. With a **Minimum Orderable Quantity (MOQ) of just ten units,** this solution is a great option for the smallest projects up to large-scale deployments. All you need to do is buy the devices, claim them and you are ready to get started.

With the TrustFLEX platform, you can order the ATECC608A-TFLXTLS secure element with a pre-established locked configuration that supports the most common cloud authentication use cases. The device comes pre-provisioned with an overwritable generic certificate for thumbprint authentication that can be replaced with your credentials for TLS-based authentication to a cloud platform. TrustFLEX also offers several other configured use cases within the same device as listed below.

It enables you to implement and fully customize secure key storage in your design. You will start with a blank ATECC608A-TCSM secure element and use our tools to configure it to meet your specific security authentication requirements. At the end of the process, you will be able to order your devices and securely provision them by leveraging our Hardware Secure Modules (HSMs) that are installed in our secure factories.

| | TRUST &GO | TRUST FLEX | TRUST CUSTOM |
|---|---|---|---|
| **Pre-configured** | YES | YES | NO |
| **Pre-provisioned** | YES | YES (flexible) | NO |
| **MOQ** | 10 units | 2000 units | 4000 units |
| **Development time** | Lowest | Lower | Custom |
| **Complexity** | Lowest | Lower | Custom |
| **Secure key Storage** | JIL High | JIL High | JIL High |

Introduction to the Trust Platform on Microchip's Youtube channel: https://youtu.be/YVtpz7d9v0o