OPTIGA™ Trust M Express and Infineon's cloud service

The easy way to securely deploy IoT devices to the cloud at scale



Introduction

OPTIGA™ Trust M Express is a pre-provisioned Secure Element that simplifies the integration of security in IoT devices.

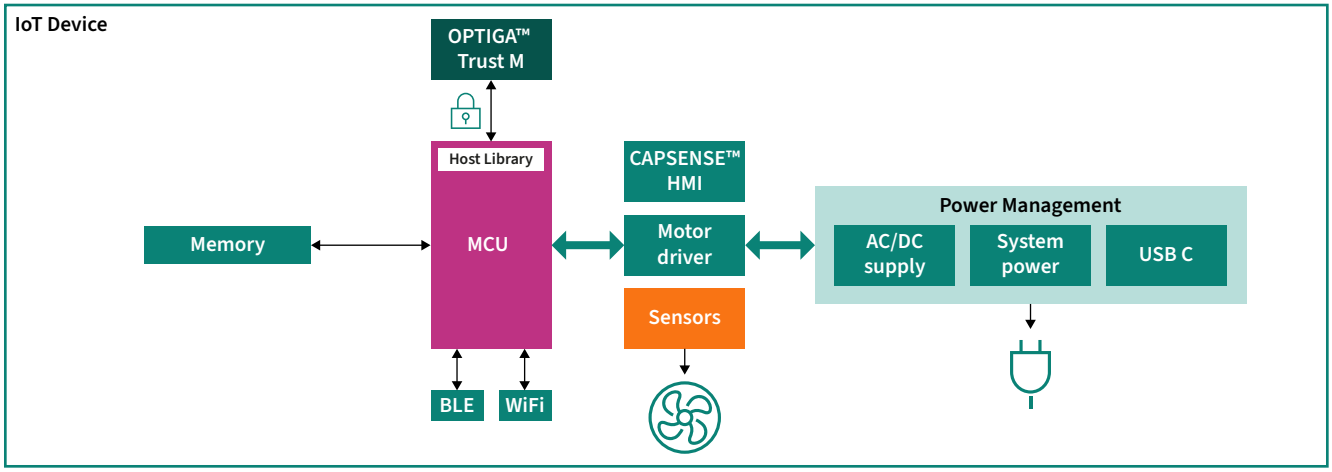
Product Features

- Pre-provisioned with ready-to-use certificates / keys for AWS multi-account registration and Azure IoT Hub pre-registration
- Infineon's cloud service support for automated provisioning of IoT devices in the product cloud
- Security controller with:
  - ECC: NIST curves up to P-521,
  - Brainpool r1 curve up to 512 bits
  - RSA with keys up to 2048 bits
  - AES key up to 256 bits, HMAC up to SHA-512
  - TLS v1.2 PRF and HKDF up to SHA-512
  - True / digital random number generators (TRNG / DRNG)
- Cryptographic toolbox commands for SHA-256, ECC and RSA features, AES, HMAC and key derivation

Product Benefits

- Off-the-shelf Secure Elements
- Ready to connect to Azure and AWS
- Automated device provisioning
- Product-to-cloud provisioning
- Simple device claiming process
- No manual intervention required
- Faster design-in process
- Easy-to-use developer kit
- NDA-free product documentation
- Robust Security

Blockdiagram



Use Cases

- Secured cloud authentication
- Secured cloud communication
- Secured software updates
- Crypto offloads

More information and tools to get started

> OPTIGA™ Trust M Express

> GitHub

BEST IN SHOW Embedded COMPUTING DESIGN embeddedworld WINNER

www.infineon.com/OPTIGA-Trust-M-Express