TRUST IoT ©

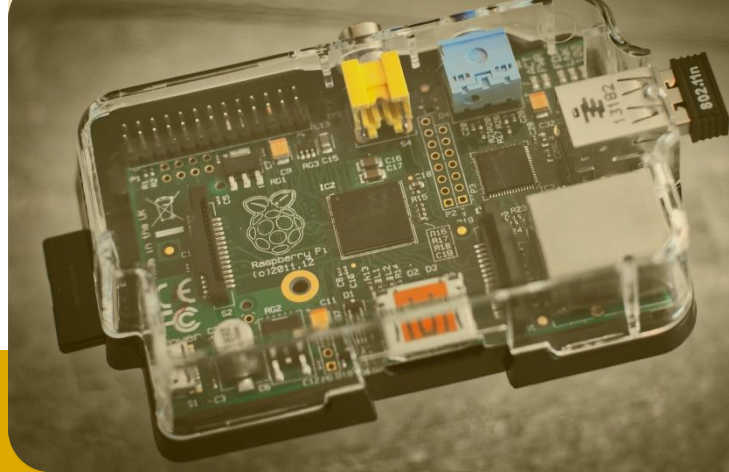### SECURE IoT NETWORK
ENSURE DATA INTEGRITY

TRUST IoT is a Secure Element to plug

on connected object ensuring trustable Chip-to-Server Data Transmission

IoT Device IDentification

TRUST IoT is a micro-controller ensuring **secure data transmission** and **object secure authentication** from object to server or cloud services.

Plugged to IoT device processor, **TRUST IoT** chip technology permits **in a single command** to get an encrypted message called Crypto-ID allowing server to:

- Authenticate the Object
- Trust Data collected on the field
- Verify message Uniqueness

Collected Data Encryption

MAIN FEATURES

- ➢ Communication Protocols:
  - o ISO/IEC 7816-3 | T=0
  - o ISO/IEC 14443-A | T=CL
- ➢ Encryption based on **AES-128** cryptography
- ➢ Transmit **up to 128 bytes** of collected data
- ➢ **MCU access conditions** (External Authenticate)
- ➢ **MSE**: Key storage and Key management
- ➢ **Dynamically computed** Crypto-ID
- ➢ Up to EAL5+ high Common Criteria HW

MAIN ADVANTAGES

- ➢ **Enrol** Device securely
- ➢ **Identify** connected objects
- ➢ **Trust** Data collected from the field
- ➢ A **single command** for:
  - o Secure authentication
  - o Data encryption
- ➢ **Easy-to-integrate** on IoT device
- ➢ End-to-End **Security from chip to server**
- ➢ Direct interaction with **RF-**Interface

Easy Integration

Optional RF- Interface

FUNCTIONAL DIAGRAM

ISO/IEC 7816-3 | T=0

Bluetooth | MQTT
Sigfox | LoRa |NB IoT

TRUST IoT APPLICATION
NATIVE OS
TRUST IoT HARDWARE

3. CRYPTO-ID

1. AUTHENTICATE MCU
2. GET CRYPTO-ID

SECURE ELEMENT

MCU

4. CRYPTO-ID

SENSOR

SERVER DATA BASE

IF NOT VERIFIED

CRYPTO –ID VERIFIED

6. DECRYPTED INFORMATION

CRYPTO-MODULE

Support for product integration

Qilium
Smartcard
Technology