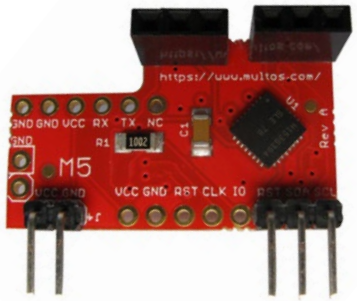
TRUST CORE



MULTOS TRUST CORE Development Kit

Security and Flexibility for Smart Devices - **Trust Core** is a member of the **MULTOS Trust Anchor** product range

MULTOS Trust Core is an embedded high-security microcontroller providing a Hardware Security Module for smart and connected devices. It offers hardware root-of-trust protection, critical for many IoT solutions and businesses.

Its flexible renowned MULTOS operating system enables a secure co-processor mode, or as a main device microcontroller. Key features allow protecting the device runtime, ensuring the identity of endpoints, securing critical data, simplifying the provisioning process, and enhanced flexibility and life cycle management. The supporting SDK reduces design effort, offers online support and contains sample application software for integrating secure connectivity using TLS/DTLS 1.2 to widely used IoT platforms such as AWS IoT. Being programmable it can support many other IoT platform solutions and bespoke security protocols. The plug-in format allows convenient integration with RasberryPi® and Arduino® single-board computers.

Functional Summary

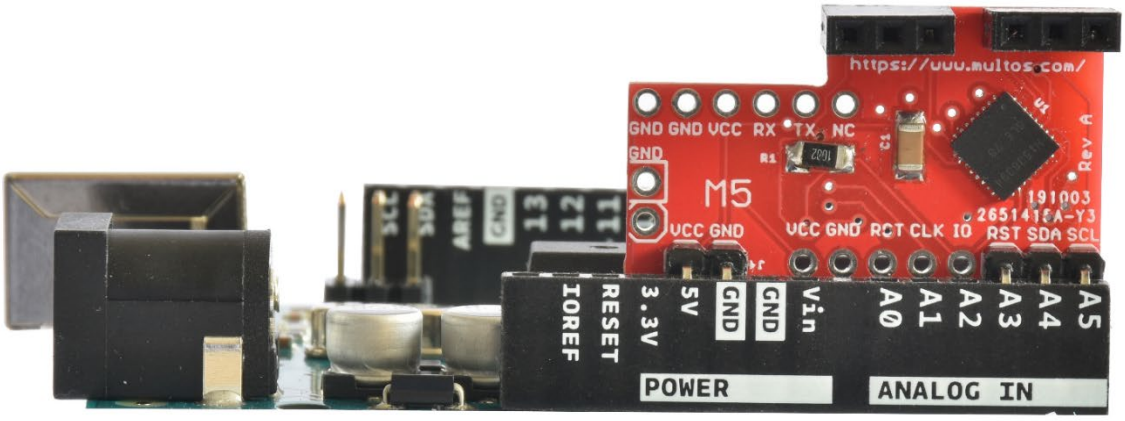
- ✓ RSA key generation & storage
- ✓ RSA signature generation & verification
- ✓ RSA encryption/decryption
- ✓ ECC key generation & storage
- ✓ ECC Diffie Hellman key agreement
- ✓ ECC DSA signature generation and verification
- ✓ TLS/DTLS 1.2
- ✓ AES key generation
- ✓ AES CBC & GCM mode encryption and decryption
- ✓ Hardware based true random number generation (TRNG)
- ✓ SHA-1 and SHA-256 hashing
- ✓ SHA-1 and SHA-256 based HMAC
- ✓ Key management functions (generation, export, import, merging)

This product has been designed for and tested with a Raspberry Pi ™ Model 3B (inc. 3B+) and Arduino™ boards compatible with the UNO R3 header layout. Use with other makes and models of board is possible (for example RPi Model 4), but please ensure that connections are compatible.

Trust Core has been designed to support AWS IoT Greengrass running on Raspbian. With its HAL and PKCS#11 library it has successfully obtained certification under the AWS Device Qualification Program.

aws qualified device internet of things

Communication with the **Trust Core** is managed by a Hardware Abstraction Layer (HAL). This ensures a consistent application programming interface across different host platforms. HAL source code is available on GitHub. On *Raspberry Pi* you can use a subset of the **standard PKCS#11 v2.40 API** (C/C++ programming) or our **TLS 1.2 API** (C/C++/Python 3 programming). Source code and documentation for both is available on GitHub. A binary distribution for Raspbian is available from the MULTOS website. Otherwise functionality is accessed via application protocol messages sent over the appropriate HAL. For a copy of the low level API document please email us at dev.support@multos.com.



Marketing Product Name	
Product name	**MULTOS TRUST CORE Development Kit**
Device characteristics	
MULTOS OS	MULTOS 4.5.3
Micro-controller	Secure operating system: MULTOS v4.5.3 (M5-P22) Secure microcontroller: Infineon SLE78CUFX5000PHM 16 bit secure microcontroller with Integrity Guard with comprehensive error detection, a self-checking dual CPU and a fully encrypted data path including encrypted calculation in the CPU
Cryptography	
Application cryptography	RNG, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, DES, 3DES, AES, SEED, RSA (up to 4096 bit keys), ECC (up to 521 bit curves)
Generic Features Supported	
AWS support	AWS IoT Greengrass running on Raspbian
Programming support	TLS 1.2 API (C/C++/Python 3 programming) PKCS#11 v2.40 (C/C++ programming) Trust Core low level API Custom secure MULTOS applications (C programming)
Compatibility	Designed for and tested with a Raspberry Pi ™ Model 3B (inc. 3B+) and Arduino™ boards compatible with the UNO R3 header

	layout. Use with other makes and models of board is possible (for example RPi Model 4), but please ensure that connections are compatible.
ISO 7816 interface	T=0, T=1, up to 447k
Application replacement	Ability to replace applications with a single ALC, new application can inherit data from the replaced application
Application support	All MULTOS M4-P18 and M5-P19 primitives supported, new embedded primitives, optimised instruction set supported
Reset pin	Reset pin for chip reset
Serial IO interface	Single transmit/receive serial port up to 57,600 baud
I2C interface	Single master and slave port
Fault processing	Ability for applications to process system faults and to halt or restart MULTOS
On-chip debugging	Full on-chip debugging when in command mode and using the SmartDeck Eclipse debugging environment (requires USB / Serial adapter).
Public size	3,200 bytes
Free RAM	9,900 bytes, shared between MULTOS and applications (session data and stack)
Free NVM for applications	At least 250K
Delays	Delay feature with optional jitter
Timers	Eight count-up and eight count-down timers
Watchdog	One hardware watchdog
Multiple power domains	Separate Vcc, GPIO and ISO power domains that support ultra-low power mode when using the ISO 14443 interface.
Security countermeasures	Extensive hardware and software security countermeasures to help protect application code and data

For full details, please visit

https://www.multos.com/dev_boards/trust_core
https://github.com/maosco/trust_core