



*The Multi-app Smartcard for EMV,
Identity and Data Security*

MULTOS

On 8, 16, 36 and 68K

MULTOS - Still the Safest Choice

Multos International's products have achieved ITSEC E6 (high) security evaluation – **the highest level of security** for any multi-application smartcard operating system. MULTOS remains the best choice for securing your data and the preferred platform for EMV, identity and data security.

Confidence of a Proven Solution

MULTOS has a proven field performance in projects ranging from EMV to transportation to large-scale national ID. This history provides assurance that MULTOS can be successfully implemented in an increasingly diverse array of smartcard projects. With over 80 million chips deployed, MULTOS is a product that is ready to roll. **Reduce the risk** in your project by using MULTOS.

MULTOS is able to run existing applications, and provide enhanced features for new applications.

Maintain Control Over your Smartcard Project

MULTOS is the only fully open smartcard scheme that gives you full control over your smartcard implementation. Fully defined lifecycle management means there is multiple sourcing at every level of the supply chain and you get to choose which parts to implement. The simple message is that MULTOS is **smartcards made easy**.

Multiply your Revenue Stream

The flexibility of a multi-application platform means that you can combine several different applications onto the one card, at any stage in the card lifecycle, along with the pre-loaded applications already installed on the MULTOS module. All this brings the chance to introduce value-add into any smartcard project.

More applications pre-loaded including M/Chip, VSDC, MODS, PKI, biometrics and loyalty.

Comprehensive Support Community

You can be certain that your smartcard project will be comprehensively supported by Multos International and the MULTOS community – your partners for success. You can choose from multiple card manufacturers, bureaux, application developers or off-the-shelf applications ranging from EMV payments, e-purse, loyalty, ID, health, biometrics, PKI and others.

New Features

The latest in the Multos International family of MULTOS implementations offer new features on the most advanced silicon platform – for continued value-for-money. MULTOS 4.2 specs, 2048-bit RSA, SEED, EMV2000 and biometric capabilities built-in; **MULTOS offers even more.**

Also available: Contactless MULTOS and MULTOS step/one for contactless payment, e-Passports, transit and more.

MULTOS

On 8, 16, 36 and 68K

Features

Implementation of MULTOS Version 4.2

Why is MULTOS considered the platform of choice for secure smartcard operating systems? Because MULTOS provides for the highest levels of privacy between multiple applications on the same card, with application firewalls ensuring the integrity and security of application-specific code and data – evaluated to ITSEC E6 (high).

Applications Pre-loaded

Multos International has combined MULTOS with a selection of the most popular applications in ROM. This saves valuable EEPROM memory for customer applications, cuts production time and reduces costs.

Application Management

The MULTOS scheme provides the issuer with full control over the applications resident on the card. This is achieved by using a secure load and delete mechanism that manages the applications on the card.

8, 16, 36, 68K EEPROM

A number of choices for EEPROM size provides space for additional applications (code and data) with the most cost effective solution for your needs. Or for even lower cost options choose MULTOS step/one with 4K & 8K.

Fast Operation

The new MULTOS 4.2 implementation from Multos International and Infineon's latest chips provides even more horsepower: faster DES and RSA cryptographic operations; application loading times of encrypted applications are even faster than previous versions – another cost benefit of MULTOS from Multos International.

Interapplication Communications

The delegation functionality enables an application to delegate commands to other applications, increasing the efficiency of MULTOS applications by removing the need to duplicate common functionality within each separate application.

Development Kit

Free SDK available for application development in 'C', java or MEL.

Efficient Memory Management

The application memory, released when applications are removed, is fragmented to give full access to available memory.

Cryptographic Capabilities

- DES**
 - Signature generation (CBC single/triple DES)
 - Encryption/decryption (ECB single DES)
- RSA**
 - Built in RSA crypto co-processor
 - RSA encryption up to 2048-bit key lengths
 - CRT calculation time of less than 150ms for 1024-bit keylengths, and less than 650ms for 2048-bit keylengths.
- SHA**
 - Calculation of message block request
 - SHA-256, AES available on request

ECC algorithms and protocols are currently in development for inclusion in our next generation of MULTOS products.

Multos International

Level 14, Zenith Tower B
821 Pacific Highway, Chatswood
2067 NSW, Sydney, Australia
Tel: +61 2 8622 9900
Fax: +61 2 8622 9999
info@multosinternational.com

Technical Specifications

CPU

Implemented

SLE66CX80PE/162PE/360PE/680PE

2.7-5.5 V operation

CC EAL5+ Certified

Clock speed: up to 7.5 MHz (external); 30 MHz (internal)

Anti-snooping mechanisms in hardware: active shields, true random number generator, counter measures against SEMA/DEMA SPA/DPA DFA, light and timing attacks

Memory

Total EEPROM: 8K, 16K, 36K, 68K

Application memory: 5.6-6.1K

Static memory: limited only by available application memory

Public: up to 530 bytes

Maximum APDU size: 291 bytes

Dynamic: up to 960 bytes

Maximum session size: 960 bytes

Applications

APIs supported: MEL V4.2

Input/Output - Contact

Protocols: T=0, T=1; PPS

Speed: Up to 223kbit/s

New Crypto features

2048-bit RSA

SEED Algorithm

Some of the Applications included in ROM

M/Chip 4 - EMV application for MasterCard (M/Chip4 and M/Chip v2 for existing systems)

MODS (MasterCard)

VSDC VIS1.4.0 - EMV application for Visa

XLS (Welcome Real-Time)

Precise Biometrics Match-on-card™

Multos International PKI

MULTOS V4.2 Specs

Default selected app

RSA key-pair generation primitive

Longer MULTOS scheme keys

Extended command set to read card details

Notes: Specifications and functionality may change