MOS *Multi-application Chip Operating System*

Founded on the latest IC technologies and our vision of the future of trusted IDs, MOS is the unequivocal smart card solution to address the convergence of the secure document, payment card, ticketing and mobile domains. It represents a new generation of true multi-application smart card operating systems.

File Manager

MOS features File Manager based on the ISO/IEC 7816 -- Identification cards -- Integrated circuit cards standard which is mandated by global standards and specifications for travel documents, driving licenses and national ID cards. The File Manager implements the standard file system and data structures, security architecture and environments, secure messaging, command set and life cycle management. Applicable standards include:

- ICAO Doc 9303 Machine Readable Travel Documents
- ISO/IEC 18013 ISO-compliant Driving Licence
- EN 419212 Electronic Identification, Authentication and Trusted Services

GlobalPlatform Card Manager

MOS actualises a GlobalPlatform Card Manager, the industry standard for provisioning and managing multiple applications on smart cards, terminals and mobile devices. The Card Manager realises the GP Environment (OPEN), Issuer (ISD) and Supplementary Security Domains (SSD), secure channel protocol (SCP) and life cycle models according to specifications. Its security architecture supports a multitude of roles and responsibilities, such as the Card Issuer, Application Provider, Controlling Authority and cardholder, and of critical importance in a multi-application card, supports complex access and privilege models with respect to individual applications.

Biometric Match-on-card

MOS supports user authentication through fingerprint biometric verification performed by the card itself. The card holder's fingerprint templates are stored within the card and the live template is sent to the card for matching and to gain access to protected files. This feature enhances user privacy, renders the card non-transferable, supports non-repudiation, provides greater entropy and dispenses with the need to remember PINs and passwords.

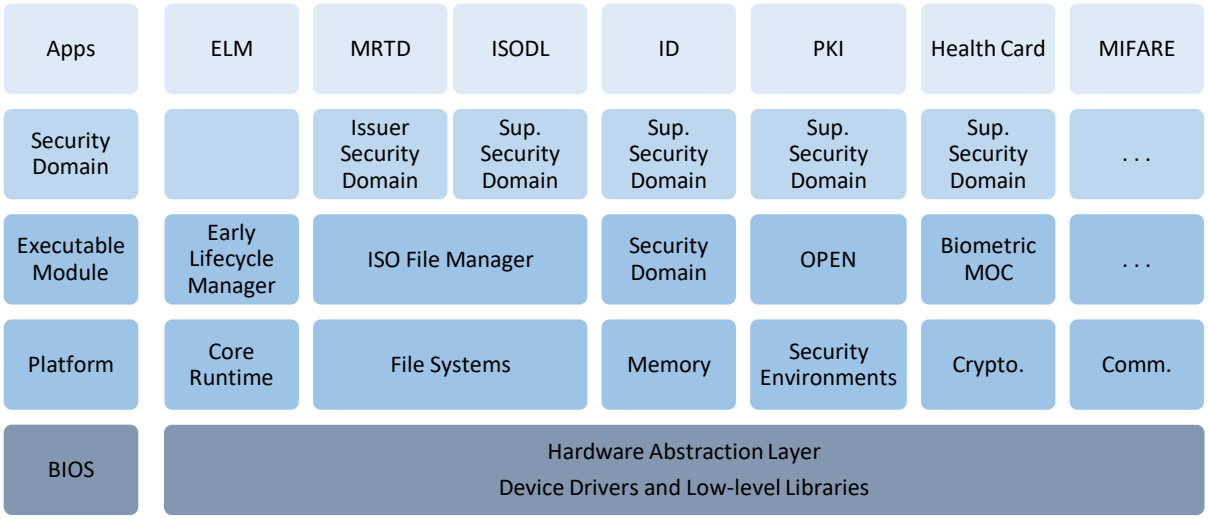
Native Implementation

Functionalities of MOS and its applications are executed entirely on the native IC platform without a virtual machine, something unique amongst multi-application COS. There are fewer modules and better code efficiency which translate to smaller memory footprint and enhanced performance in keeping with the design objectives of storing more applications and faster transactions.

Early Lifecycle Manager

When MOS has been flashed onto the IC and is powered for the first time, it is in the early lifecycle or Initialisation state. During this phase, the ELM Application allows card manufacturers to customise the MOS product according to the target project and application where external factors like the smart card terminals, card antenna design, software application and security risks determine the operating conditions of MOS.

Block Diagram

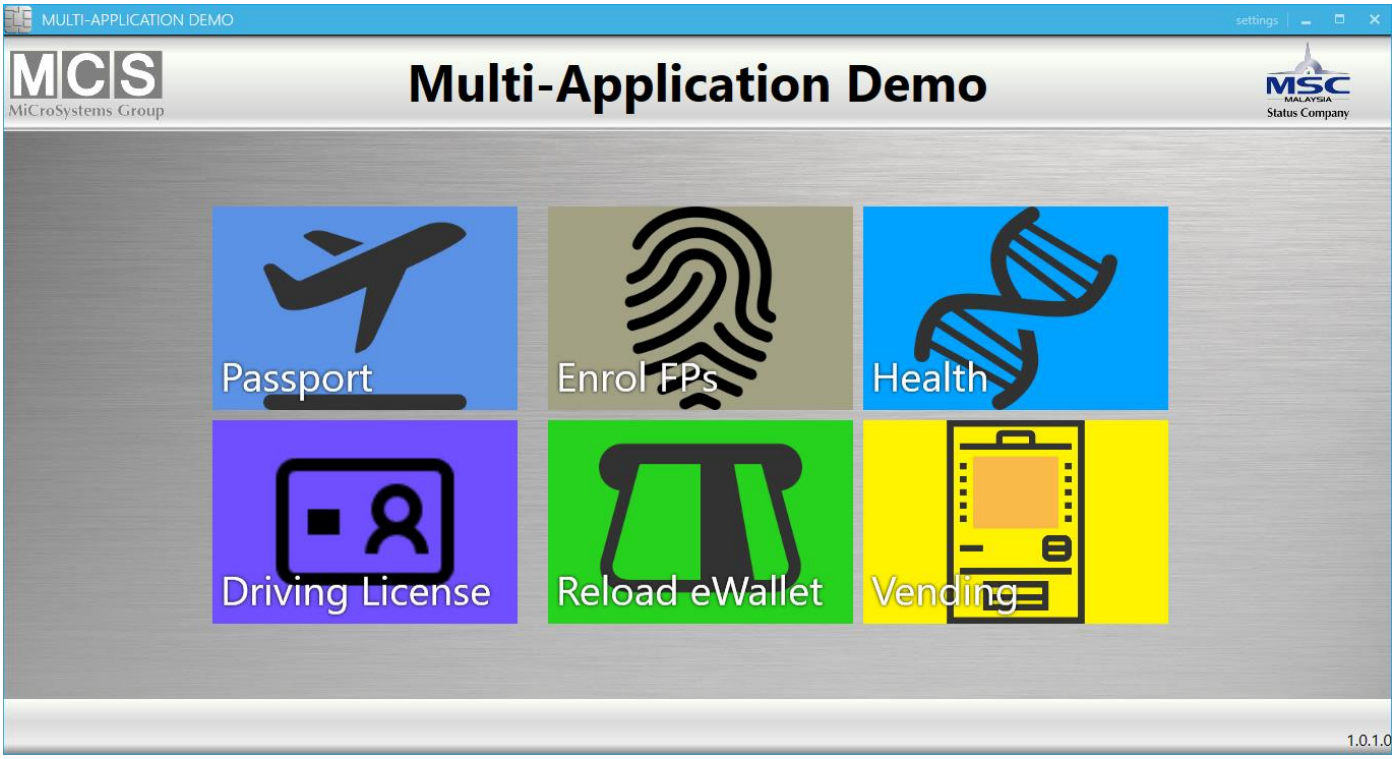


MCS Microsystems Sdn Bhd (469491-P) http://www.mcs-group.com.my Tel: +60 3 8996 9168
4th Floor IRIS Smart Technology Complex, Technology Park Malaysia, Bukit Jalil, 57000 Kuala Lumpur, Malaysia.

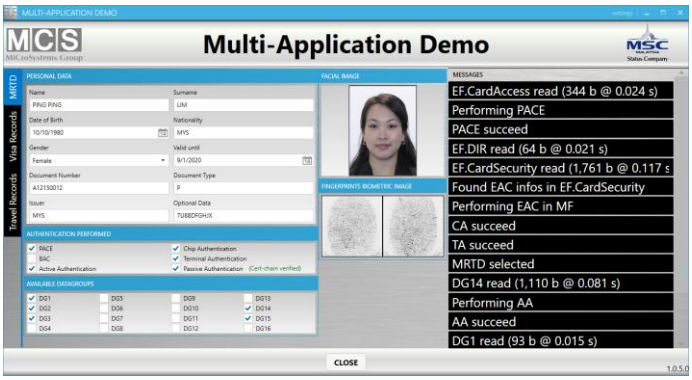
Multi-Application Demo Software

An application software is available to demonstrate the functionalities of the MOS smart card. It executes on a Windows PC and requires a PC/SC contact and/or contactless smart card reader and a fingerprint scanner (see User Manual for compatible models).

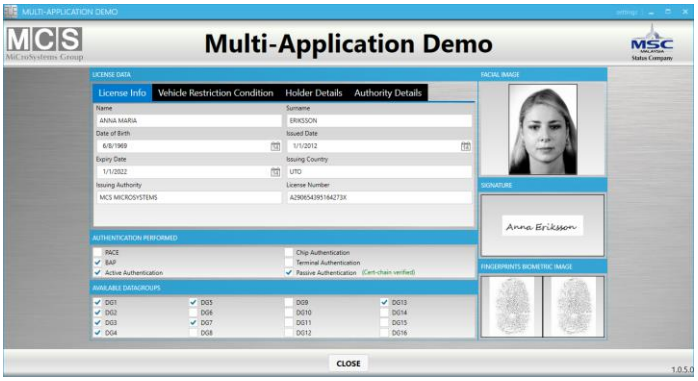
Main Screen



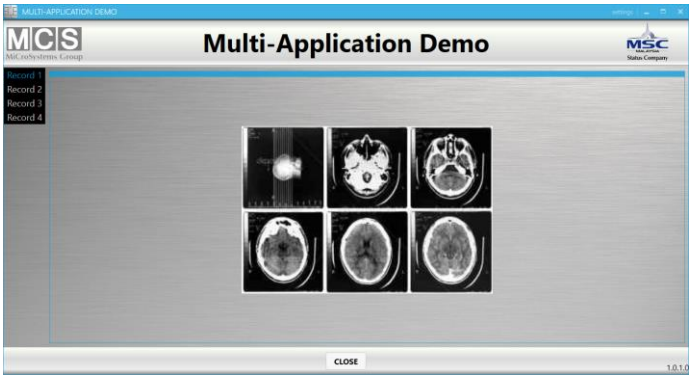
E-Passport Screen



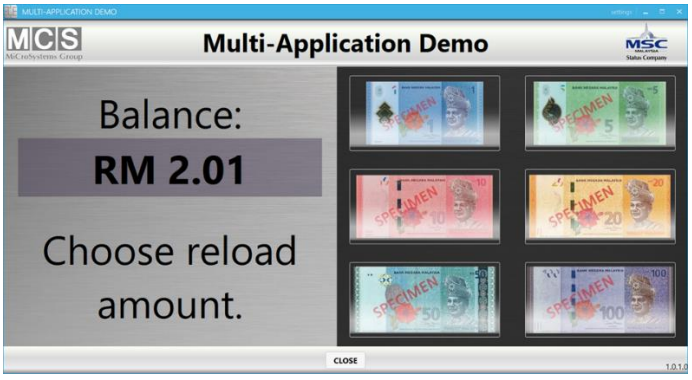
E-Driving License Screen



Health Card Screen



E-Purse Screen



Specifications

Passport	ICAO Doc 9303, Machine Readable Travel Document, 7th Ed., 2015 Basic Access Control Supplemental Access Control PACE (GM, CAM, ECDH, TDES, AES, CAN, MRZ) Active Authentication (RSA, ECDSA) Chip Authentication (ECDH, TDES, AES) Terminal Authentication (ECDSA, SHA-2) CVCA migration : elliptic curve domain parameters and key sizes LDS2 Travel Records, Visas and Additional Biometrics
Driving License	ISO/IEC 18013 ISO-compliant Driving License File structure Basic Access Protection (TDES) Active Authentication (RSA, ECDSA) Extended Access Control EACv1 (ECDH, ECDSA, TDES, AES, SHA-2) PACE (GM, ECDH, TDES, AES)
Secure Signature	EN 419212 Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services Digital signature RSA PKCS#1 v1.5 and ECDSA Complete and partial on-card hashing with SHA-1, SHA-2 Data decipherment service
MIFARE	MIFARE® DESFire® EV2 up to 16KB MIFARE Plus® EV1 up to 4KB (including MIFARE Classic®)
File Manager	ISO/IEC 7816 Identification cards -- Integrated circuit cards File system: MF, DF, EF, DO, Application DF (7816-4) Standard command set (7816-4) Secure messaging and PIN / password authentication (7816-4) Security architecture and security environments (7816-8) Life cycle management (7816-9)
GP Card Manager	GP Card Specifications ver. 2.3 GP Environment (OPEN) Issuer Security Domain (ISD), Supplementary Security Domain (SSD) Executable load file (ELF), executable module (EM), Application Four logical channels Life cycle models : application (un)locking, card termination Content installation / removal, and access control rules Secure channel protocol SCP02 – i = '15' and '55' Trusted framework Privileges : card lock, card terminate, trusted path, authorised management, global delete, global lock, global registry, final application
Early Lifecycle Manager	Contact communication protocols configuration Contactless communication protocols configuration Card production life cycle (CPLC) data configuration Lifecycle management (Restore; Lock; Install ISD) Security mechanism configuration
Biometric match-on-card	ISO/IEC 19794-2:2005 – Information technology – Biometric data interchange formats – Part 2: Finger minutiae data ISO/IEC 19785-1:2006 – Common biometric exchange formats framework – Part 1: Data element specification ISO/IEC 7816-11:2004 -- Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods High interoperability with most of the template generators available on the market AFIS-grade accuracy and MINEX III compliant High tolerance to distortion and sensor variations, invariant to translation, configurable rotation tolerance up to 180° and suitable for small sensors

Security	SPA, DPA, SEMA, DEMA, fault-injection countermeasures Retry counter, usage counter and delay Anti-tearing and anti-bypass mechanisms Atomic write function
Cryptography	AES : 128, 192 and 256 bits DES : 56, 112 and 168 bits RSA : up to 2,048 bits ECC : up to 521 bits (prime field) SHA-1, SHA-224, -256, -384 and -512 True random number generator (AIS-31)
Communication	Contact : ISO/IEC 7816-3, T=0 and T=1, up to 600 kbps Contactless : ISO/IEC 14443 Type A / B, up to 848 kbps, VHBR up to 6.8 Mbps; ISO/IEC 18092 NFC passive card mode Parameter and protocol selection (PPS) Extended length APDU, up to 1,024 bytes
Compliance	BSI TR-03105 Conformity Tests for eMRTD Application Protocol and Logical Data Structure Common Criteria EAL 4+ - MRTD with EAC and PACE protection profile GlobalPlatform Compliance Test Program (upon customer request) EMVCo Card Level 1 Protocol (upon customer request)
Development Tools	SDK and APDU scripts for chip initialisation, pre-/personalisation processes Multi-application Demo for passport (ICAO LDS2) and driving license (ISO/IEC 18013). PKI middleware with PKCS#11 API and Windows Smartcard Minidriver

Multi-platform

MOS is available on the STMicroelectronics ST31 family of secure microcontrollers. It will be available on the NXP P71D321 family and others in future.

STMicroelectronics ST31P450 IC	ARM® SecurCore® SC000™ 32-bit RISC core 10 Kbytes of User RAM 450 KB of Flash memory (210 KB of user data memory) Contact assignment compatible with ISO/IEC 7816-3 standards, 2.7 V to 5.5 V supply voltages Contactless ISO/IEC 14443 Type A, EMVCo™ and ISO/IEC 18092 passive mode standards Automatic CPU frequency adaptation for optimum power consumption Three-key Triple DES accelerator and AES accelerator AIS-31 Class PTG.2 compliant true random number generator (TRNG) NESCRYPT coprocessor for public key cryptography algorithm ISO/IEC 13239 CRC calculation block CC EAL6+ and EMVCo certification
NXP P71D321 Platform IC	MRK3-SC 16/32-bit RISC (reduced instruction set computing) CPU 12 KB of user RAM Full flash memory solution up to 344 KB. Up to 500 KB non-volatile memory available ISO/IEC 7816 contact interface; standard data rates up to TA1 = 97h ISO/IEC 14443 contactless interface – Type A interface for data rates up to 848 kbit/s Fully certified symmetric, hash and asymmetric cryptography libraries. Up to RSA 4096 bits and ECC 640 bits key length. MIFARE® DESFire® EV2 up to 16KB and MIFARE Plus® EV1 up to 4KB (including MIFARE Classic®) EMVCo and CC EAL 6+ (PP 0084 with loader package 2)