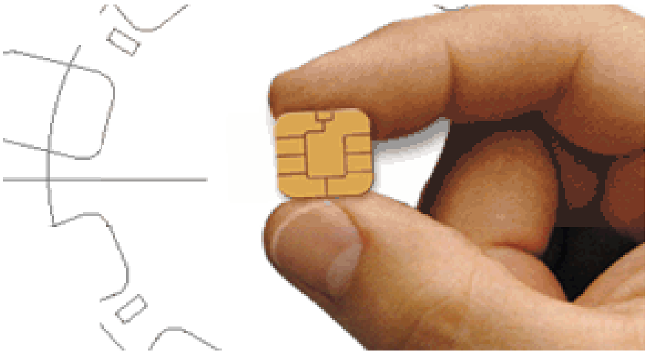
MCS
MiCroSystems Group

SMOSCC

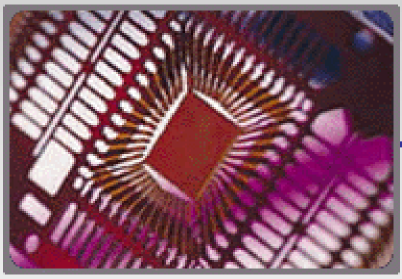
Small Machine Operating System Common Criteria



SMOSCC is a smart card operating system purpose-designed for national ID application which also serves as an ideal platform for national e-passport, precisely meeting the individual needs of each and every country.

SMOSCC has its foundation in the chip operating system that was selected for the first multi-application national ID smart card in the world. Throughout its twelve year history, SMOSCC and its earlier versions have been deployed on devices from various IC manufacturers on a range of products with up to 80KB user memory and with contact, contactless and/or USB interfaces.   More than 25 million smart cards are in circulation world-wide, proving its effectiveness in combating identity theft everyday.

A multi-application operating system, SMOSCC simultaneously supports multiple applets with custom instruction sets and data structures from several agencies on a single smart card, limited only by the IC specifications. Imagine a national ID card with a host of other functions like driver's permit, PKI token, e-purse, frequent traveler card and so forth, which simplifies its cardholder's dealings with various public and private agencies



APPLICATION MANAGEMENT

- Dynamic, post-issuance applet loading and deletion.
- Digital certificates control the loading and deletion of applets, and card retirement on a card-by-card or scheme wide basis.
- Applets can be encrypted in whole or in part for security reason.
- Secure firewalls between card applets protect confidential data and sensitive operations.
- Garbage collection reclaims unused memory after object deletion.

KEY FEATURES

- Efficient "Small Machine" application runtime environment is common across all chip platforms.
- Applets can be executed on all SMOSCC smart cards regardless of IC model like 'plug-and -play'
- Sophisticated security architecture on-card and off-card.
- Efficient memory management.
- Four logical channels for true multi application transactions.

Trademarks and copyrights enclosed herein are properties of their respective companies.
MCS shall not be liable for any loss or damage arising from the use of any information in this document or any error or omission in such information

ON-CARD MODULES

SMOSCC smart cards are available with a host of applets and native libraries that can be utilised to meet your project needs.

ICAO E-PASSPORT

Applet compliant with the ICAO Document 9303 for biometric passports supporting the Logical Data Structure (LDS) and security features, such as Active Authentication (AA), Basic Access Control (BAC), Extended Access Control (EAC) and Password Authenticated Connection Establishment (PACE). Lifecycle management is controlled by security keys or Secure Access Modules (SAM). Fast performance with retrieval speed of 13KB/s or 11KB/s with BAC.

PKI

The PKI Applet enables the SMOS smart card to be used as a PKI token. Its key features are:

- RSA key pair generation and storage.
- Certificate generation for signing purpose,
- 3DES session keys creation.
- PKCS #1, #10, #11 and #15.

MATCH-ON-CARD FINGERPRINT BIOMETRICS

For privacy reason, fingerprint biometrics verification can be performed within the smart card using our match-on-card native library licensed from our technology partners. Minutiae and pattern matching are available.

PROTON R3 E-PURSE

One of the most widely used domestic e-purse applet developed by Proton World.

ICOS

IRIS file management client-server applet with client sizes from 4KB through 64KB. ICOS is patented by and developed for IRIS Corporation Berhad.

Please check with us for actual product configuration.

DEVELOPMENT TOOLS

Comprehensive and easy-to-use set of development tools, including assembler, symbolic debugger and card loader.

Applets are written in Small Machine language, like a stack-oriented assembly language.

Build your own native library for use by third-party applets.

SPECIFICATIONS*

ISO/IEC 7816 CONTACT INTERFACE

- Communication speeds of 115200 bps max.
- ISO 7816-3, T=0 byte-oriented protocol
- Operating voltages of 3V and 5V

ISO/IEC 14443 CONTACTLESS INTERFACE

- Type B protocol
- Communication speeds of 848 kbps max.
- 256-byte frame size

CRYPTOGRAPHY

- TDES: 64, 128 and 192-bit key lengths
- AES: 128, 192 and 256-bit key lengths
- RSA: Maximum 2,048-bit key length, straight-forward and CRT, encryption and key generation.
- ECC Elliptic Curve Cryptography
- SHA: SHA-1, SHA-2 message digest, 521 bits.
- Security countermeasures against SPA, DPA and DFA.

* Depending on IC

PRODUCT FAMILY

ST23YL80	80 KB	T=0	
	RSA, ECC, DES, SHA-1		
ST23YR80	80 KB	T=0 / CL	EAL4+
	RSA, ECC, DES, AES, SHA		

ENQUIRY
MCS Microsystems Sdn Bhd
IRIS Smart Technology Complex
Technology Park Malaysia
Bukit Jalil, 57000 Kuala Lumpur, Malaysia
Tel. +603 8996 9168 Fax. +603 8996 3168

Trademarks and copyrights enclosed herein are properties of their respective companies.

MCS shall not be liable for any loss or damage arising from the use of any information in this document or any error or omission in such information