Advanced Card Systems Ltd.
Card & Reader Technologies

ACOS5-64 Cryptographic Smart Card

Functional Specifications V1.01

info@acs.com.hk
www.acs.com.hk

Table of Contents

List of Figures

List of Tables

1.0. Introduction

This document aims to describe the features and functions of the ACS Smart Card Operation System Version 5.0 64 kilobytes version (ACOS5-64) as developed by Advanced Card Systems Ltd.

ACOS5-64 is an advanced cryptographic smart card that fully complies with ISO 7816 Parts 1, 2, 3, 4, 8 and 9, and is specially designed for public-key-based applications. In addition, the card is intended for enhancing security and performance of RSA public-key cryptographic operations that are essential in smart card Public Key Infrastructure (PKI) and high-level security requirements.

Furthermore, ACOS5-64 supports a number of security infrastructures and applications, including:

- Crypto-API and PKCS #11 Middlewares
- Smart Card Minidriver
- Domain Smart Card Logon
- Secure Online Certificate Generation
- Outlook, Windows Mail, Outlook Express and Mozilla Thunderbird mail signing and encryption (S/MIME)
- Encrypting File System (EFS)
- Mozilla Firefox
- Internet Explorer
- Microsoft VPN/Open VPN
- OpenID
- IIS SSL
- Adobe Acrobat
- Lotus Notes
- Netscape
- SSH

2.0. Symbols and Abbreviations

Abbreviations	Description
3DES	Triple DES
AES	Advanced Encryption Standard
AMB	Access Mode Byte
AMDO	Access Mode Data Object
APDU	Application Protocol Data Unit
AT	Authentication Template
ATR	Answer to Reset
CBC	Cipher-Block Chaining Mode of Encryption
CCT	Cryptographic Checksum Template
CT	Confidentiality Template
CLA	Class byte of ISO 7816 APDU
CRT	Control Reference Template
CSP	Cryptographic Service Provider
DES	Data Encryption Standard
DF	Dedicated File
DST	Digital Signature Template
ECB	Electronic Code Book Mode of Encryption
EEPROM	Electrically Erasable Programmable Read-Only Memory
EF	Elementary File
EF1	PIN File
EF2	KEY File
FCP	File Control Parameters
FDB	File Descriptor Byte
XXh	Hexadecimal representation of a byte.
HT	Hashing Template
IIS	Internet Information Services
INS	Instruction byte of ISO 7816 APDU
ISO	International Organization for Standardization
Lc	Length of command data of ISO 7816 APDU
LCSI	Life Cycle Status Integer
Le	Length of expected response data of ISO 7816 APDU
LSb	Least Significant Bit
LSB	Least Significant Byte
MAC	Message Authentication Code
MF	Master File

Abbreviations	Description
MSb	Most Significant Bit
MSB	Most Significant Byte
P1	Parameter 1 of ISO 7816 APDU
P2	Parameter 2 of ISO 7816 APDU
P3	Parameter 3 (Lc or Le) of ISO 7816 APDU
RFU	Reserved for Future Use
ROM	Read-Only Memory
RSA	Public key cryptographic algorithm by Rivest, Shamir and Adleman
SAC	Security Attribute – Compact
SAE	Security Attribute – Expanded
SCB	Security Condition Byte
SCDO	Security Condition Data Object
SE	Security Environment
SFI	Short File Identifier
SHA	Secure Hash Algorithm
SM	Secure Messaging
SW1SW2	ISO 7816 return Status Word from the card
TLV	Tag-Length-Value
UQB	Usage Qualifier Byte
Var.	Variable Length
||	Concatenation of bytes

Table 1: Symbols and Abbreviations

2.1. Features

ACOS5-64 Cryptographic Smart Card features the following highlights:

- Full 64 KB of EEPROM for Application Data
- Fast EEPROM Writing Speed
- File system that can reuse deleted files' memory space without compromising security
- File system that manages the EEPROM to prolong the card's life span
- Compliance with ISO 7816 Parts 1, 2, 3, 4, 8, 9
- High Switchable Baud Rate Support from 9600 to 223200 bps
- ISO 7816 part 4 file structures support: Transparent, Linear Fixed, Linear Variable, Cyclic
- Mutual Authentication with Session Key Generation
- On-board RSA key generation of up to 4096 bit
- AES-128/192/256 support
- Secure Messaging ensures data transfers are confidential and authenticated
- Common Criteria EAL5+ (Chip Level)
- FIPS 140-2 Compliance
- Multi-level Secured Access Hierarchy
- Anti-tearing Function Support
- Backward compatibility mode available so the card may be used as an ACOS5-32 card

2.2. Technical Specifications

ACOS5-64 Cryptographic Smart Card has the following technical characteristics:

2.2.1. Electrical

- Operating Voltage: 5 V DC +/-10% (Class A) and 3 V DC +/-10% (Class B)
- Maximum Supply Current: < 20 mA
- ESD Protection: ≤ 5 KV

2.2.2. EEPROM

- Capacity: 64 KB (65, 536 bytes)
- EEPROM Endurance: 500K erase/write cycles
- Data Retention: 10 years

2.2.3. Environmental

- Operating Temperature: -25 °C to 85 °C
- Storage Temperature: -65 °C to 150 °C

2.3. Answer-to-Reset (ATR)

After hardware reset (e.g. power up), the card transmits an Answer-to-Reset (ATR) in compliance with ISO 7816-3. ACOS5-64 supports the protocol type T=0 in direct convention. For full description of ATR options, see ISO 7816-3. The ATR may be completely changed using the ATR file.

2.4. Cryptographic Capabilities

ACOS5-64 Cryptographic Smart Card supports a number of cryptographic capabilities including:

- DES and Triple DES with 64/128/192 bit keys data encryption in ECB and CBC mode. AES 128/192/256-bit is also supported
- Secure on-card RSA key pair generation with 512-bit to 4096-bit keys in 256-bit steps
- RSA signature computation and verification with 512-bit to 4096-bit keys in 256-bit steps
- RSA card verifiable certificate with 512-bit, 768-bit and 1024-bit key signed certificate
- Private and secret key file read access can be set to “Never”
- Mutual authentication (terminal-to-card and card-to-terminal) using Triple DES with session key generation for encryption and MAC
- SHA-1 and SHA-256 message hashing
- Secure Messaging function for confidential and authenticated data transfers
- File access condition capability with ISO 7816 compliant Secure Attribute - Compact. File access is only allowed if the proper security conditions are met (e.g. PIN submission)
- Command execution condition capability per Dedicated File (DF) with ISO 7816 compliant Secure Attribute - Extended. Commands are allowed only if the proper security conditions are met (e.g. PIN submission)
- FIPS 140-2 compliant hardware based random number generator

3.0. Card File System (User Files, Structures and Usage)

ACOS5-64 has a dynamic file system wherein memory wear and tear is properly managed to prolong its life span. The card operating system organizes, manages and administers the function of the card.

The fundamentals of the ACOS5-64 File System consist of the following:

- Card Life Cycle
- Card Header Block
- Hierarchy of Files on ACOS5-64 Cards
- File Types
- File Header Data
- File Life Cycle
- Predefined File Identifiers
- Limitations of the File System
- Anti-tearing and Roll-forward Mechanisms

3.1. Card Header Block

The card header block is a special memory area accessed by the card operating system for its operation.

3.2. File Header Block

ACOS5-64 organizes the user EEPROM area by files. Every file has a File Header Block, which is a block of data that describes the file's properties. Knowledge of the file header block will help the application developer for the file creation and accurately plan for the usage of the EEPROM space.

3.3. Hierarchical File System

ACOS5-64 is compliant with ISO 7816-4 file system and structure. The file system is very similar to that of the modern computer operating system. The root directory of the file system is the Master File (MF). Each application or group of data files in the card may be contained in a directory called a Dedicated File (DF). Each DF and MF may store data in their respective Elementary Files (EF), as shown in **Figure 1**.

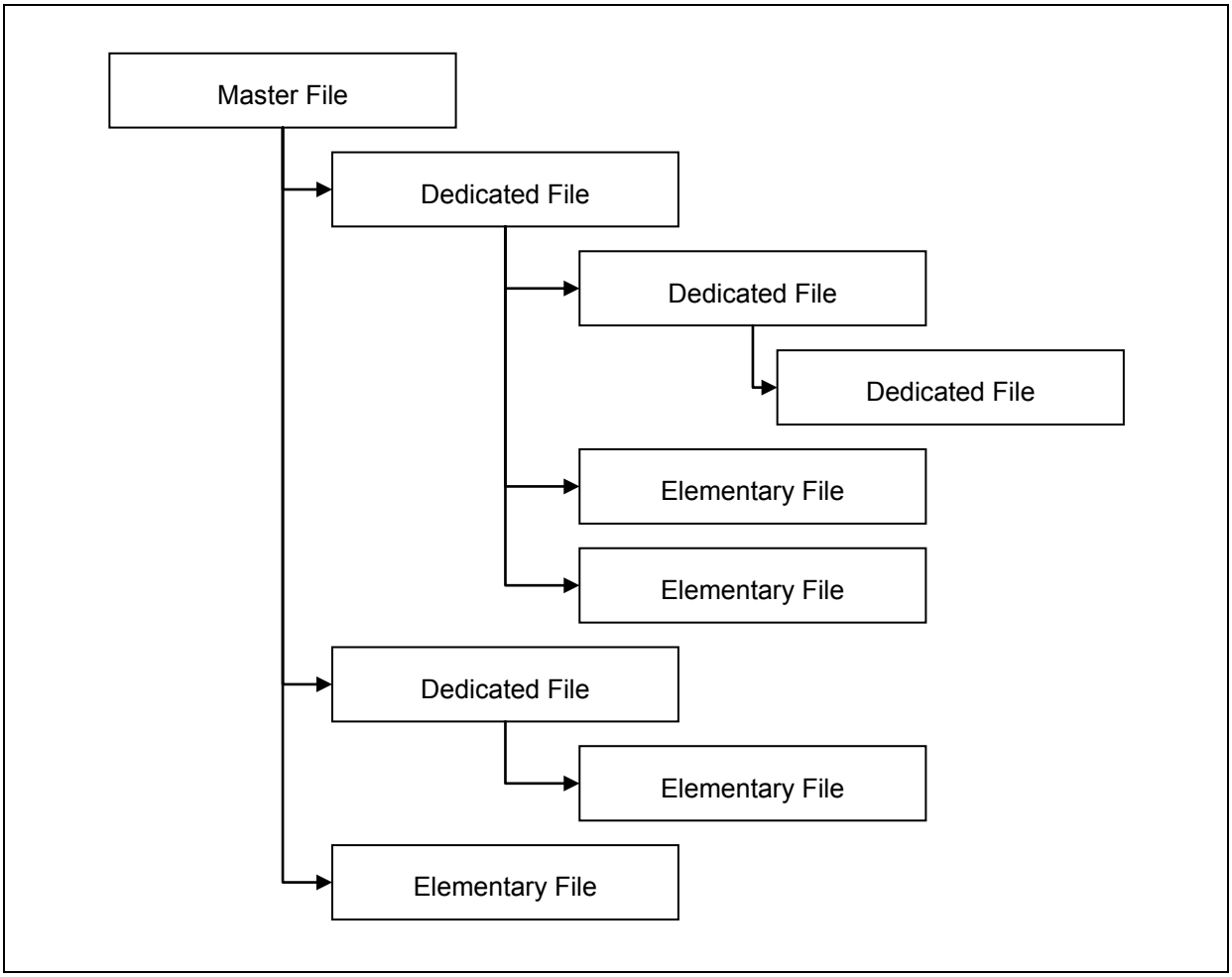

Figure 1: File System Hierarchy according to ISO 7816-4

3.4. File Life Cycle

ACOS5-64 files have four states during its life cycle. The figure below illustrates how it works:

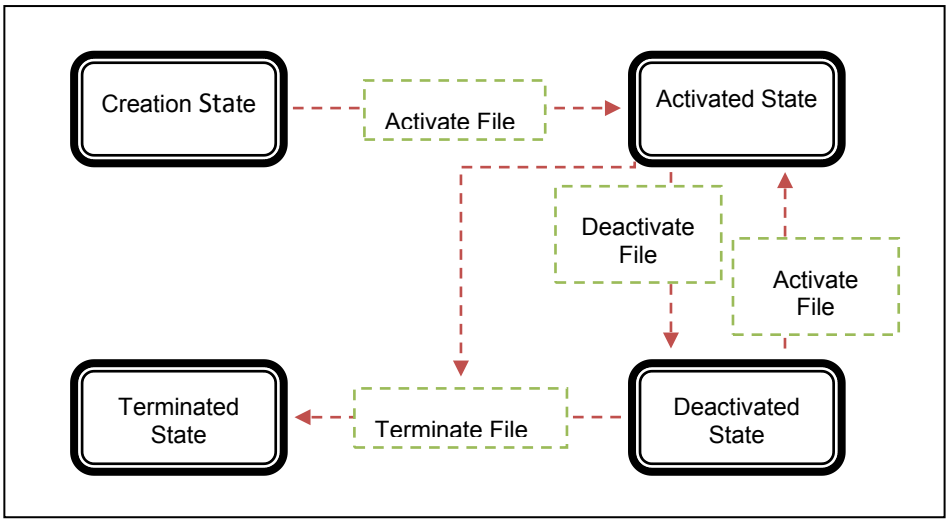

Figure 2: File Life Cycle States

- In Creation/Initialization states, all commands to the file will be allowed. After personalization, it is important to ACTIVATE the files to bring the card to operational state. This will enforce each file's security conditions.
- In Activated state, commands to the file are allowed only if the file's security conditions are met.
- In Deactivated state, only most commands to the file are not allowed except SELECT FILE, ACTIVATE FILE, DELETE FILE, and TERMINATE DF/EF.
- In Terminated State, all commands to the file will not be allowed.

3.5. Predefined File Identifiers

There are few predefined File IDs. Since these are file identifiers that are implicitly know by the card operating system, they cannot be used for other files.

3.6. Anti-tearing Mechanism

ACOS5-64 uses a mechanism called *anti-tearing* in order to protect the card from data corruption due to card tearing (i.e., card suddenly pulled out of reader during data update, or reader suffer mechanical failure during card data update). Immediately on the next card reset or power up, ACOS5-64 applies the necessary data recovery if tearing is detected. In such case, the operating system will return the corrupted data to its original state before the card tearing occurred.

3.7. Roll Forward Mechanism

ACOS5-64 uses a mechanism where unfinished tasks are continued after a power interruption or card tearing. On reset, ACOS5-64 checks the roll-forwarding fields and does the necessary continuation of interrupted commands.

3.8. Card Life Cycle

ACOS5-64 has the following card stages during its life cycle:

0. Manufacturer Stage
1. Transport Stage
2. Issuer Stage
3. Transport Stage
4. Personalization Stage
5. User Stage

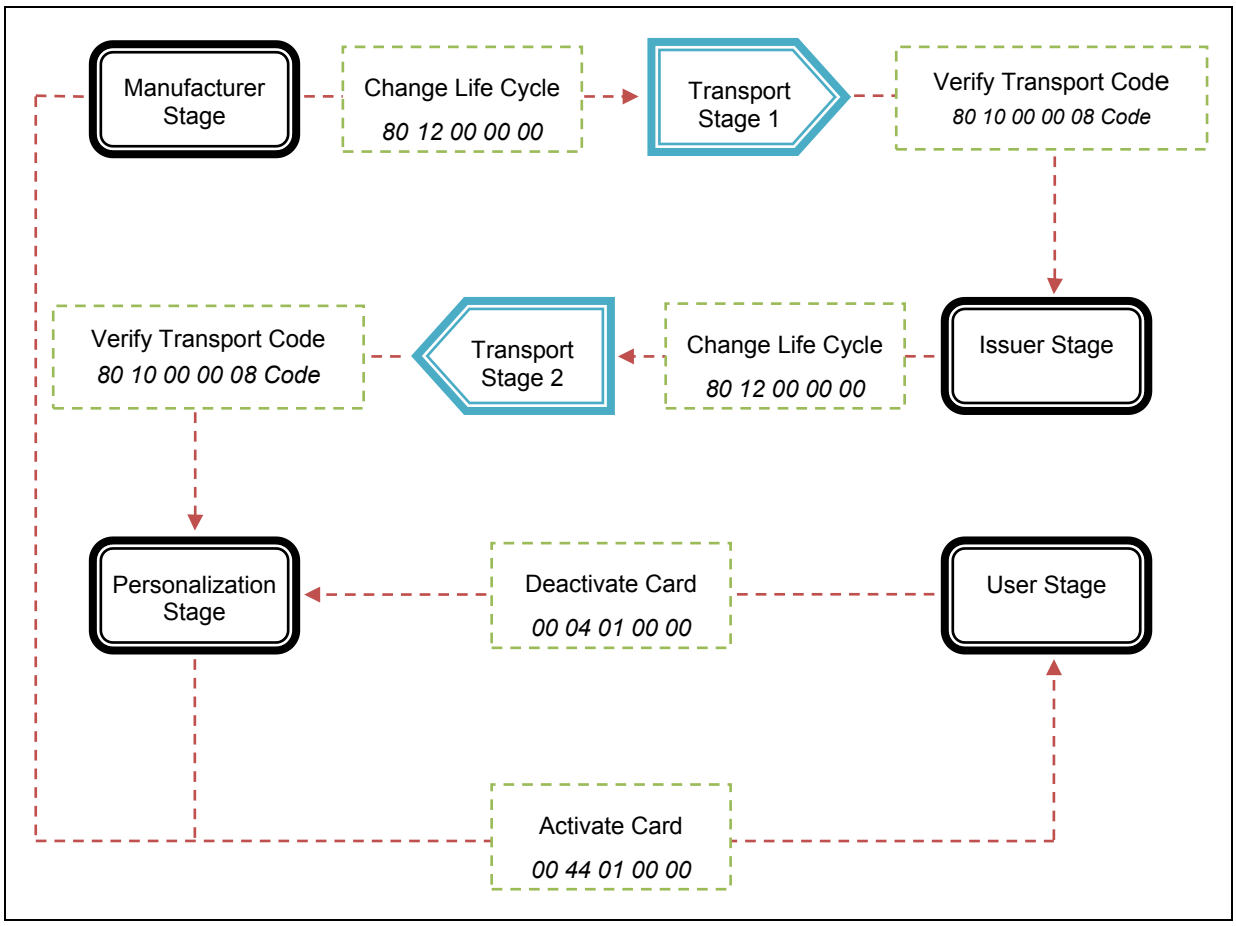

Figure 3: Card Life Cycle Stages

3.8.1. Manufacturer Stage

This stage is the initial state of the card. ACS factory or the application developer is allowed to freely access the card header block. The card header block can be referenced by its address using the READ BINARY or UPDATE BINARY command.

Note: *ACS may add customized commands for the customer at this stage. ACOS5-64 remains at this stage as long as: (1) It is not activated from this stage; and (2) the Card Life Cycle has not been changed to the Issuer Stage. All commands are allowed in this stage. The ACOS5-64 does not allow going back to this stage once the life cycle is changed.*

3.8.2. Transport Stage

The Transport Stage should be activated when the card is being transported. The only command that may be used is the VERIFY TRANSPORT CODE command. After successfully submitting the transport key, the state of the card will be change to the next applicable state.

3.8.3. Personalization Stage

The successful submission of the *transport key* from the Issuer Stage grants access to a user at this stage. ACOS5-64 users can no longer directly access the card header block as in the previous stage. Users can create and test files created in the card as if in Operational Mode. This stage is used for personalizing the card to a specific user like loading of names, etc. The ZEROIZE CARD USER DATA command is allowed in this stage (unless the Zeroize Card User Data Disable Flag is set - see **Section 3.2.4**).

Note: *Customized commands cannot be loaded at the User or Personalization Stage. The card cannot go back to Manufacturer Stage or Issuer Stage.*

Deleting Custom Commands is not allowed in the Personalization Stage and User Stage.

3.8.4. User Stage

The card goes into this stage once the card is activated. ZEROIZE CARD USER DATA command is no longer allowed. Sending the DEACTIVATE CARD command deactivates the card and life cycle stage goes back to the Personalization Stage.

4.0. Card Internal Files – Structure and Usage

This is to illustrate the internal files of the ACOS5-64 card along with its structure and usage:

- Card Holder Verification File
- Symmetric Key File
- RSA Private Key and Public Key File
- Purse File
- Security Environment File

4.1. Internal Card Holder Verification (CHV) File

A CHV file is an Internal Linear-fixed elementary file. This file is used by the card operating system to store PIN records for cardholder verification. Essentially, a DF or MF shall have only one CHV file. This file, when under a DF, is considered to store local PINs or PINs that are relevant within the DF only. When under a MF, this file stores global PINs or PINs that are relevant throughout the whole card file hierarchy.

4.2. Internal Symmetric Key File

A Symmetric Key file is an Internal Linear-Variable Elementary File. This file is used by the card operating system to store symmetric key records for cryptographic use. Symmetric keys are used by symmetric-key algorithms such as DES, 3DES, and AES for cryptographic operations. Essentially, a DF or MF shall have only one symmetric key file. This file is considered to store local keys or keys that are relevant within the DF only, when under a DF. When under a MF, this file stores global keys or keys that are relevant throughout the whole card file hierarchy.

4.3. Internal RSA Key File

A RSA Key File is an internal transparent file with an FDB of 0x09h. This file holds a single RSA key that could be either a “Private Key” or a “Public Key”. A MF/DF is allowed to have multiple RSA Key Files within the capacity of the EEPROM.

4.4. Internal Purse File

Purse files are Internal Cyclic Files. An ACOS5-64 Purse File should always have record length of 16, and number of records must at least be 3. The first 2 physical records store information on the purse, while the rest are used to store transactions records (LOG).

4.5. Internal Security Environment File

A Security Environment (SE) File is an Internal Linear Variable EF that stores Security Environments in the form of SE templates. Every DF shall have a designated SE File whose file ID is indicated in the parent DFs header block. An SE file can have up to 15 identifiable records.

5.0. Card Access Rights and Security (Environment and Usage)

This chapter illustrates the access rights and security capabilities of the ACOS5-64 card along with its environment and usage. They are:

- File Security Attributes
- Security Environment
- Control Reference Templates
- Mutual Authentication Procedure
- Session Key Generation

Commands are restricted by ACOS5-64 depending on the target file's (or current DFs) Security Access Conditions. These conditions are based on PINs and KEYs being maintained by the system. Card Commands are allowed if certain PINs or KEYs are submitted or authenticated.

Global PINs are PINs that reside in a PIN EF (EF1) directly under the MF. Likewise, local keys are KEYs that reside in a KEY EF (EF2) under the currently selected DF. There can be a maximum of 31 Global PINs, 31 Local PINs, 31 Global Keys, and 31 Local Keys at a given time.

5.1. File Security Attributes

Each file (MF, DF, or EF) has a set of security attributes in its headers. There are two types of security attributes the ACOS5-64 uses, namely, Security Attribute Compact (SAC) and Security Attribute Expanded (SAE).

5.2. Security Environment

Security conditions are coded in a Security Environment File. Every DF has a designated Security Environment File or SE File, whose file ID is indicated in the DF's header block. Each SE record has the following format:

<Security Environment ID Template> <Security Environment DO Template>

5.3. Control Reference Templates

5.3.1. Authentication Template

The *Authentication Template* defines the security condition that must be met for this SE to be satisfied. The security conditions are either PIN or Key authentications.

5.3.2. Cryptographic Checksum Template (CCT)

Cryptographic Checksum Template (CCT) defines which parameters to use in computing for the MAC, which is used in Secure Messaging and/or PSO.

5.3.3. Confidentiality Template (CT)

Confidentiality Template (CT) defines which parameters to use in encrypting or decrypting data in Secure Messaging and/or PSO. This template is also applied to asymmetric encryption/decryption.

5.3.4. Digital Signature Template (DST)

Digital Signature Template (DST) defines which parameters to use in asymmetric key-related operations.

5.3.5. Hash Templates (HT)

Hash Template (HT) defines which parameters to use in PSO-HASH.

5.4. Authentication

Mutual Authentication is a process in which both the card and the card-accepting device verify that the respective entity is genuine. A *Session Key* is the result of a successful execution of mutual authentication. The session key is only valid during a session. A *session* is defined as the time after a successful execution of the mutual authentication procedure and a reset of the card of the execution of another mutual authentication procedure. The execution of a SELECT FILE command also ends a session.

5.5. Secure Messaging

Secure Messaging (SM) allows secured communication between the terminal/server backend an ACOS5-64, which supports secure messaging for authentication and confidentiality.

There are two modes of SM that can be applied in two different security levels. The first mode is *SM for authenticity* (SM-sign) the other is *SM for confidentiality* (SM-enc). The SM modes will be applied to both the command and response data.

6.0. Life Support Application

These products are not designed for use in life support appliances, devices or systems, where malfunctions of these products can reasonably be expected to result in personal injury. ACS customers using or selling these products for use in such applications do so on their own risk and agree to fully indemnify ACS for any damages resulting from such improper use or sale.

7.0. Contact Information

For additional information, please visit http://www.acs.com.hk.

For sales inquiry, please send an email to info@acs.com.hk.