Advanced Card Systems Ltd.
Card & Reader Technologies

ACOS5-64 v3.00 Cryptographic Card

Backward Compatibility Guide V1.00

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

Table of Contents

1.0. Introduction 3
2.0. Comparison of ACOS5 card versions 4
2.1. ACOS5-64 Command Compatibility Guide 5
3.0. Change to Non-FIPS mode (64K mode) 6

List of Tables

Table 1 : Comparison of ACOS5 card versions 4
Table 2 : ACOS5-64 Command Compatibility Guide 5

1.0. Introduction

This document describes the differences of ACOS5 card versions and guides you in using ACOS5-64 v2.00 and ACOS5-64 v3.00 Non-FIPS mode (sometimes referred to as 64K mode in this document). Similarly, this guide will help you migrate from using CryptoMate64 token to CryptoMate Nano (in Non-FIPS Mode) token.

2.0. Comparison of ACOS5 card versions

The following table shows a comparison of the two ACOS5 versions:

Specifications	ACOS5-64 v2.00	ACOS5-64 v3.00
Memory	64 KB	64 KB
Cryptographic Capabilities	DES/3DES 56/112/168-bit AES 128/192/256-bit RSA 512-bit to 4096-bit SHA1 and SHA 256	DES/3DES 56/112/168-bit AES 128/192/256-bit RSA 512-bit to 4096-bit SHA1 and SHA 256
Modes of Operation	• 64 KB mode (default)	• FIPS 140-2 mode (default) • Non-FIPS mode (or 64K mode) • NSH-1 mode

Table 1: Comparison of ACOS5 card versions

The default mode of the ACOS5-64 v3.00 is FIPS 140-2 mode as delivered from factory. In FIPS 140-2 mode, the card is limited to FIPS 140-2–approved capabilities like RSA Key Generation 2048-bit and 3072-bit keys, Triple DES 168-bit and SHA-256. Non-approved capabilities like RSA Key Generation 1024-bit and 4096-bit, DES and Triple DES 112-bit, and SHA1 are disabled in FIPS 140-2 mode.

In the Non-FIPS mode or also called as 64K mode, all cryptographic capabilities as stated in **Table 1** are usable. For backward compatibility to applications currently using ACOS5-64 v2.00, the ACOS5-64 v3.00 must be set to Non-FIPS mode.

Note: *The card contents are cleared when changing mode of operation.*

2.1. ACOS5-64 Command Compatibility Guide

The table below shows a comparison of card commands of ACOS5-64 v2.0 and ACOS5-64 v3.0 Non-FIPS mode (64K mode).

Command/Function	ACOS5-64 v2.00 64 KB mode	ACOS5-64 v3.00 Non-FIPS mode (64K mode)
Answer To Reset	3B BE 96 00 00 41 05 20 00 00 00 00 00 00 00 00 90 00h	3B BE 96 00 00 41 05 30 00 00 00 00 00 00 00 00 90 00h
RSA Key Pair Generation	Supports CRT and Non-CRT key pair generation	Supports CRT key pair generation
Get Card Info	Serial Number (6-byte) APDU: 80 14 06 00 06h	Serial Number (8-byte) APDU: 80 14 06 00 08h
Get Card Info – Card OS Version APDU: 80 14 06 00 08h	Card OS Version: 41 43 4F 53 05 02 00 40 90 00h	Card OS Version: 41 43 4F 53 05 03 01 40 90 00h
Get Card Info – Operation Mode Byte APDU: 80 14 09 00 00h	Not supported	Returns: 95 XX, where XX means: 00h – FIPS 140-2 mode 01h – Emulated 32 KB mode 02h – Non-FIPS or 64K mode 10h – NSH-1 mode
Get Card Info – Verify FIPS Compliance APDU: 80 14 0A 00 00h	Not supported	Returns 90 00h if compliant or 6F XX for non-compliance
Get Card Info – PIN Authentication State APDU: 80 14 0B [PIN ID] 00h	Not supported	Returns 01h if PIN is authenticated, and 00h if not.
Get Card Info – Key Authentication State APDU: 80 14 0A [Key ID] 00h	Not supported	Returns 01h if Key is authenticated, and 00h if not.

Table 2: ACOS5-64 Command Compatibility Guide

3.0. Change to Non-FIPS mode (64K mode)

The script below changes the mode of operation of the ACOS5-64 v3.00 card into Non-FIPS mode (64K mode).

```
;Clear Card
80 30 00 00 00 (9000)

;Set to Non-FIPS mode (64K mode)
00 D6 C1 91 01 02 (9000)

.Reset

;Get Card Info - Mode of operation
80 14 09 00 00 (9002)
```