Advanced Card Systems Ltd.
Card & Reader Technologies

ACOS5-64 FIPS 140-2 Level 3 Security Policy

Version 1.15

Advanced Card Systems Ltd.
Unit 2010 – 2013, 20th Floor
Chevalier Commercial Centre
8 Wang Hoi Road, Kowloon Bay
Hong Kong

Table of Contents

List of Figures

List of Tables

1.0. Introduction

This document defines the non-proprietary Security Policy for Advanced Card Systems Ltd.'s ACOS5-64 single-chip cryptographic module (CM), submitted for verification in accordance to Federal Information Processing Standards Publication 140-2 (FIPS PUB 140-2) for overall Security Level 3 single-chip standalone hardware module requirements.

The security policy is required for FIPS 140-2 validation and is intended to be part of the package of documents that are submitted to Cryptographic Module Validation Program (CMVP). It describes the capabilities, protection, and access rights provided by the cryptographic module. It also contains a specification of the rules under which the module must operate in order to be in FIPS mode. The security policy allows individual and organizations to determine whether the cryptographic module meet their security requirements.

The primary purpose of this device is to provide data security and authentication for government and enterprise personnel. The module is specifically designed to resist non-evident tampering by both physical and electronic means.

The CM is a single integrated circuit chip containing an operating system and its data security and authentication application in its firmware.

1.1. Scope

This document covers the secure operation of ACOS5-64 including initialization, roles, and responsibilities of the operating the product in a secure, FIPS-compliant manner.

1.2. Security Level

The cryptographic module meets the overall requirements applicable to Level 3 security of FIPS 140-2. The detail of the security level met by this cryptographic module for each security requirement is as follows:

Security Requirements	Level
1. Cryptographic Module Specification	3
2. Module Ports and Interfaces	3
3. Roles, Services, and Authentication	3
4. Finite State Model	3
5. Physical Security	3
6. Operational Environment	N/A
7. Cryptographic Key Management	3
8. EMI/EMC	3
9. Self-Tests	3
10. Design Assurance	3
11. Mitigation of Other Attacks	N/A

Table 1 – FIPS 140-2 Security Level Met by ACOS5-64

1.3. References

[VE-ACOS5-64] *ACOS5-64 FIPS 140-2 Vendor Evidence.* Version 1.05. Advanced Card Systems Ltd. October 2015

[AIS31] *Functionality classes and evaluation methodology for true (physical) random number generators*. Version 3.1

[SP800-90A] *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*. NIST Special Publication 800-90A. January 2012

[FIPS186-3] *Digital Signature Standard (DSS),* Federal Information Processing Standard Publication 186-3. June 2009

[REF-ACOS5-64] *ACOS5-64 Reference Manual*. Version 2.05. Advanced Card Systems Ltd. October 2015

1.4. Glossary

Abbreviations	Description
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
BOM	Bill of Material
CBC	Cipher-Block Chaining Mode of Encryption
CCT	Cryptographic Checksum Template
CT	Confidentiality Template
CLA	Class byte of ISO 7816 APDU
CM	Cryptographic Module
COS	Card Operating System
CRT	Control Reference Template
CSP	Critical Security Parameter
DES	Data Encryption Standard
DF	Dedicated File
DRBG	Deterministic Random Bit Generator
DST	Digital Signature Template
ECB	Electronic Code Book Mode of Encryption
EEPROM	Electrically Erasable Programmable Read-Only Memory
EF	Elementary File
EMI	Electromagnetic Interference
EMC	Electromagnetic Compatibility
FCP	File Control Parameters
FDB	File Descriptor Byte

Abbreviations	Description
XXh	Hexadecimal representation of a byte
HT	Hashing Template
IART	ISO 7816 Asynchronous Receiver/Transmitter
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
MSb	Most Significant Bit
MSB	Most Significant Byte
MSDN	Microsoft Developers Network
NIST	National Institute of Standards and Technology
NDRNG	Non-Deterministic Random Number Generator
P1	Parameter 1 of ISO 7816 APDU
P2	Parameter 2 of ISO 7816 APDU
P3	Parameter 3 (Lc or Le) of ISO 7816 APDU
PCB	Printed Circuit Board
PCBA	PCB Assembly
PC/SC	Personal Computer/Smart Card Standard
PKCS	Public Key Cryptographic Standard
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
SO	Security Officer

Abbreviations	Description
SW1 SW2	ISO 7816 return Status Word from the card
TLV	Tag-Length-Value
TRNG	True Random Number Generator
UQB	Usage Qualifier Byte
Var.	Variable length
||	Concatenation of bytes

Table 2 – Abbreviations

2.0. Cryptographic Module Specification

ACOS5-64 is a hardware cryptographic module validated against the FIPS 140-2 at Security Level 3. It is a two-factor authentication smart card module. It provides digital signature creation/verification for online authentication and data encryption/decryption for online transactions. The user's private and public key pairs can be generated and stored on the chip. ACOS5-64 has 64 kilobyte of EEPROM for storage of these cryptographic keys and other critical security parameters. Additionally, the private key can never be exported. The implementation of FIPS-Approved cryptographic algorithms is in accordance to Cryptographic Algorithm Validation Program (CAVP).

Figure 1 – ACOS5-64 Module

2.1. Cryptographic Boundary

ACOS5-64 is a single-chip cryptographic module. The cryptographic boundary of ACOS5-64 module is the edge of the chip itself. Its integrated circuit chip module includes both the hardware and firmware.

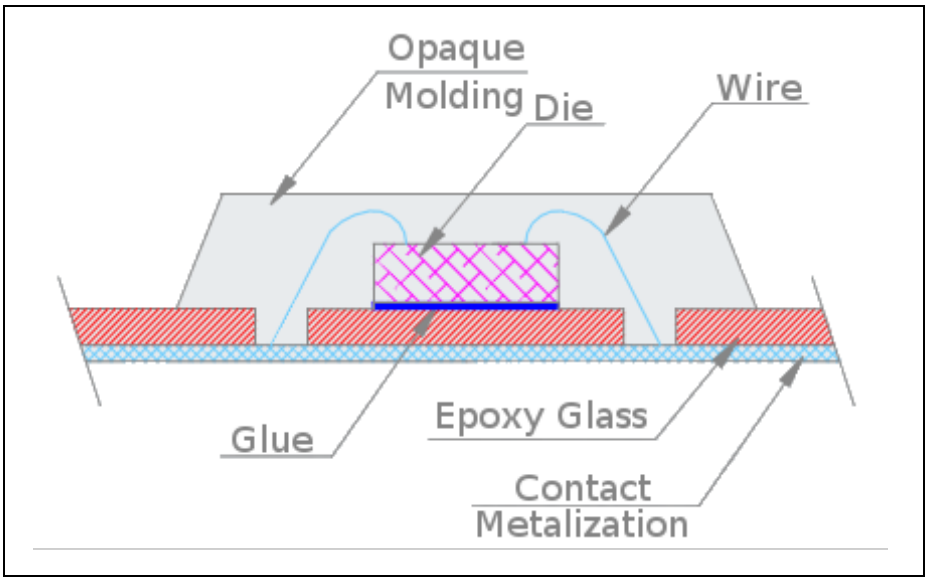

Figure 2 – Cross-Sectional Cryptographic Boundary of ACOS5-64

As stated, the cryptographic boundary is the edge of the chip itself. Thus, compromises of other components connected to it cannot comprise the module and its CSPs.

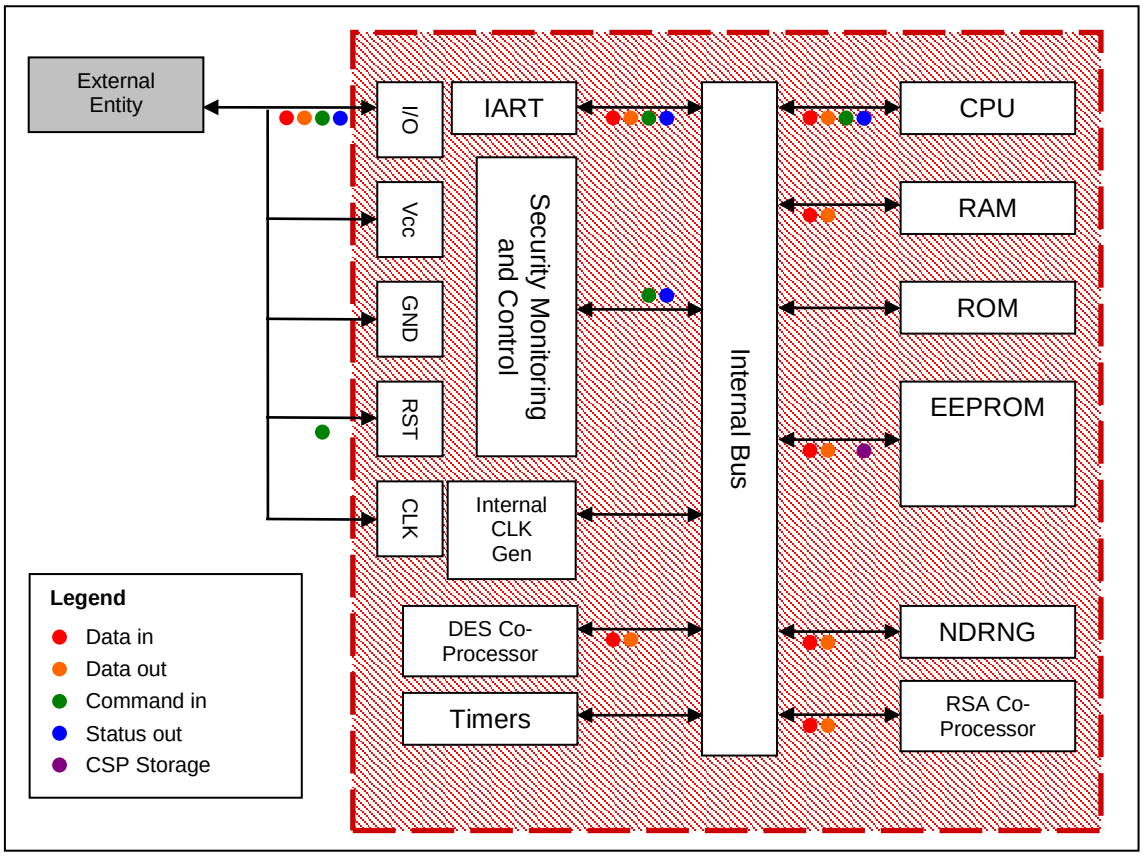

Figure 3 – Cryptographic Boundary

2.2. Hardware

ACOS5-64 includes an STMicroelectronics ST23YL80 HW integrated circuit. This IC provides a low-power, high-performance 8/16bit CPU core with ROM program memory, EEPROM code or data memory, and cryptographic accelerator.

ST23YL80 contains a Next Step Cryptography accelerator (NESCRYPT) to enable efficient computation for GF(p) arithmetic for RSA. NESCRYPT also includes dedicated operators to accelerate SHA-1 and SHA-2 implementations.

The EDES accelerator is also used to perform quick Triple DES operations.

ST23YL80 also contains a Non-Deterministic Random Number Generator (NDRNG) which is used to argument the Deterministic Random Number Generator used for CAVP.

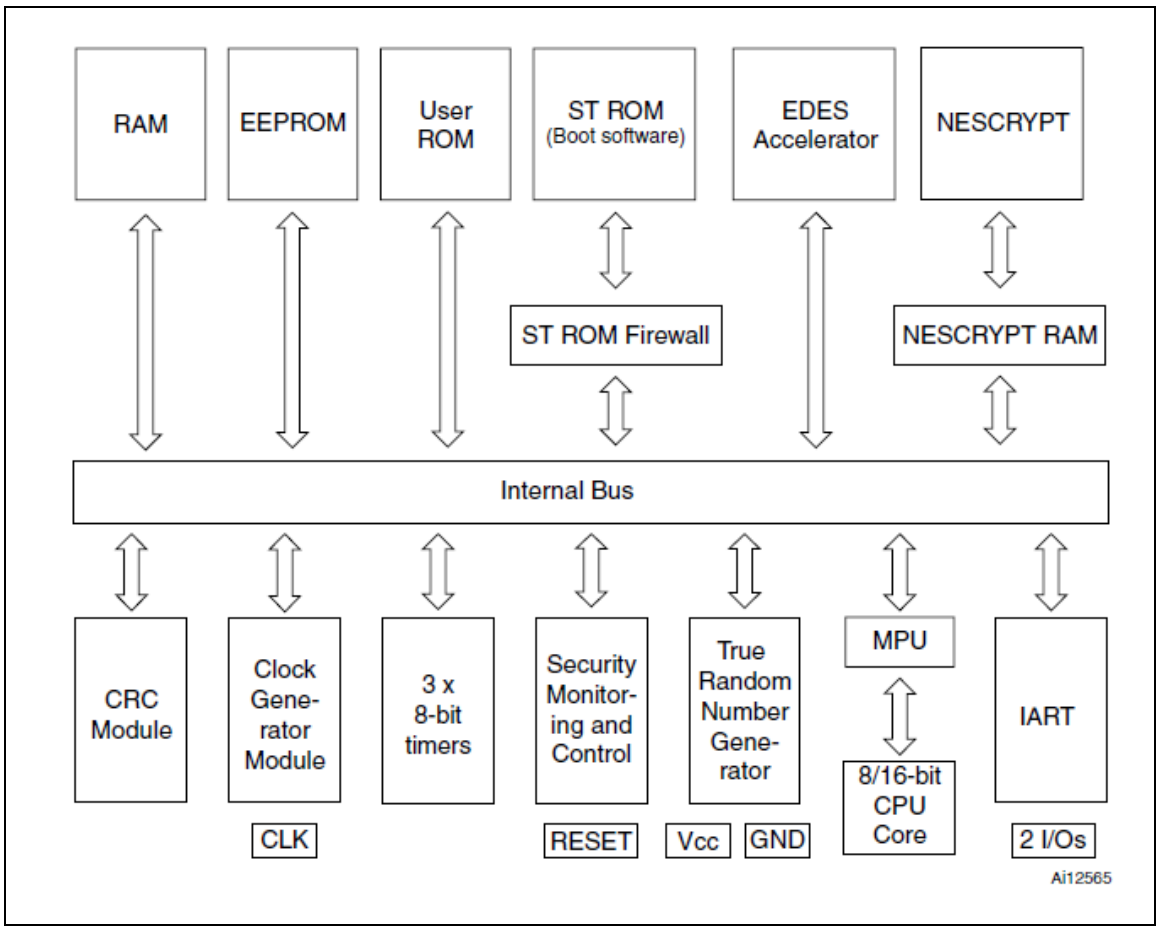

Figure 4 – ST23YL80 Block Diagram

2.3. Firmware

The firmware version for the FIPS 140-2 Level 3 Certified is 3.00.

All software components of the modules including the operating system and supported cryptographic algorithms are embedded in the User ROM area as part of the Smart Card Operating System (COS). This COS firmware is masked into the IC card chip of the module.

The ACOS5-64's chip implements all CSP and symmetric and asymmetric keys.

The AES algorithm and RSA key generation are implemented in the firmware, while all other supported cryptographic algorithms are implemented in the NESCRYPT library, which uses the ST23YL80's crypto co-processor.

Note: *The FIPS–certified product can also be referred to as: ACOS5-64 v3.00 in some ACS documents.*

2.4. Modes of Operation

The ACOS5-64 module running version 3.00 of the firmware can only operate in FIPS mode after being securely initialized.

2.4.1. Secure Initialization

In order for the module to function under FIPS mode, certain files need to be created and initialized to ensure that security conditions and roles are properly set. For more details, please refer to the ACOS5-64 Reference Manual, **Section 9 – FIPS Mode File System Requirements**.

2.4.2. FIPS-mode of operation

ACOS5-64 implements a list of FIPS-Approved algorithms as shown in **Table 3**.

Algorithm	Certificate Number(s)	Mode of operation	Security Functions
Triple-DES	Triple-DES Cert. #1982	ECB, 112[1]/168-bit Keys	Encryption/Decryption
		CBC, 112[1]/168-bit Keys	
Triple-DES MAC	Triple-DES Cert. #1982, vendor affirmed	168-bit Keys	Sign/Verify
AES	AES Cert. #3539	ECB, 128/192/256-bit Keys	Encryption/Decryption
		CBC, 128/192/256-bit Keys	
RSA Key Generation	RSA Cert. #1816	2048/3072-bit Keys	Key Generation
RSA Signature Generation	RSA Cert. #1816 and CVL Cert. #591	2048/3072-bit Keys	Sign (PKCS#1 with SHA-256 Hashing)
RSA Signature Verification	RSA Cert. #1816 and CVL Cert. #591	2048/3072/4096-bit Keys	Verify (PKCS#1 with SHA-256 Hashing)
SHA-1	SHA Cert. #2917	Byte-oriented	Hashing Operation
SHA-256	SHA Cert. #2917	Byte-oriented	Hashing Operation
DRBG	DRBG Cert. #893	Hash_DRBG using SHA256	Random number generation

Table 3 – ACOS5-64 FIPS 140-2 Approved Algorithms and Security Functions

ACOS5-64 also supports a Non-Approved FIPS 140-2 algorithm when running in FIPS mode. This is shown in **Table 4** below.

[1] 112-bit keys are not used as part of any service

Algorithm	Mode of operation	Security Functions
NDRNG	AIS31 Compliant	Entropy input for DRBG
Triple-DES Key Wrapping	168-bit Keys	Key Wrapping (Triple-DES Encryption and Triple-DES MAC)

Table 4 – ACOS5-64 FIPS 140-2 Non-Approved Algorithm in FIPS-mode

2.4.3. FIPS Mode Indicator

Upon factory initialization, the header block of ACOS5-64 is set for it to operate in FIPS mode directly.

ACOS5-64 provides a command to query whether the module is functioning under FIPS mode. Issuing the Get Card Info command using Verify FIPS Compliance as parameter will return a Success indicator if the module is currently functioning in FIPS mode, and a corresponding error code otherwise. See the reference manual for more information.

3.0. Cryptographic Module Ports and Interfaces

ACOS5-64 restricts all information flow and physical access. The physical and logical interfaces define all entry and exit points to and from this cryptographic module.

3.1. Physical Ports

ACOS5-64 provides the physical interfaces following the ISO 7816 Parts 2 (Dimensions) and 3 (Electrical standards). The location of the contacts for this cryptographic module is shown in the figure below:

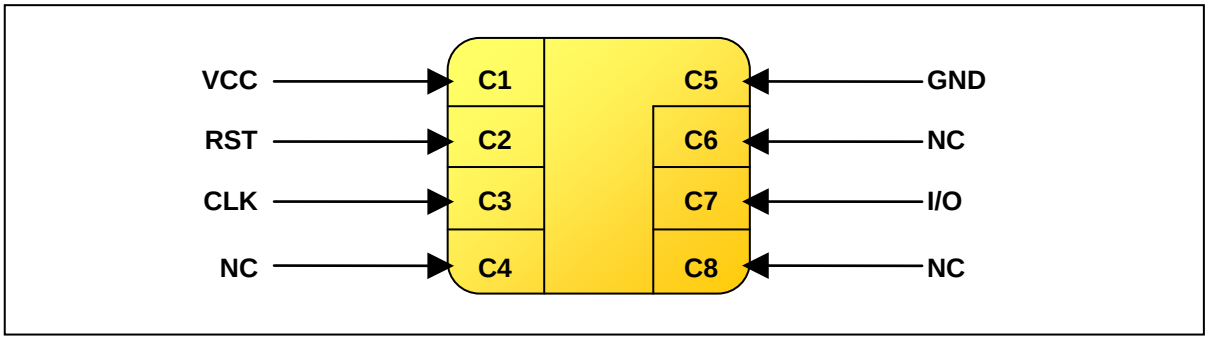

Figure 5 – Contact Plate Physical Interface for ACOS5-64

There are five electrical signals transmitted to the module through the external entity. These electronic signals are in full compliance with the ISO 7816 Part 3 standard and is enumerated below:

Electrical Signals	Contacts	Description
Power Supply Input	**VCC**	Voltage supply of 2.7 V to 5.5 V
Reference Voltage	**GND**	Ground
Reset Signal	**RST**	External; supplied from the interface device
Clocking/Timing Signal	**CLK**	External communication clock signal from 1 MHz to 5 MHz
Serial Data	**I/O**	Input/output for serial data to/from the processor
Not Connected	**NC**	These ports C4, C6, C8 are not used

Table 5 – ACOS5-64 Electrical Signals Description

ACOS5-64 supports the protocol type T=0 in direct convention and up to 256 bytes of data can be exchanged through one APDU command.

3.2. Logical Interfaces

Once the communication between the other entity (e.g. smart card reader) and ACOS5-64 is established, the latter functions as a slave processor to process and respond to the other entity's commands.

ACOS5-64 adheres to a well-defined set of state transitions. Within each state, a specific set of commands is accessible. The module provides the following logical interfaces:

Logical Interface	Physical Port	APDU Command Fields
Data Input	I/O Pin	Command data field
Data Output	I/O Pin	Response data field

Logical Interface	Physical Port	APDU Command Fields
Control Input	I/O Pin	CLA INS P1 P2
Status Output	I/O, CLK, and RST Pins	SW1 SW2
Power Input	Vcc Pin and GND Pin	

Table 6 – Logical Interfaces for ACOS5-64

ACOS5-64 does not have a bypass capability.

4.0. Roles, Services, and Authentication

This cryptographic module supports authorized roles for operators and corresponding services within each role.

4.1. Roles

The following table summarizes the authorized roles for operators that are supported by ACOS5-64:

Role	Description
Card Holder ***(User Role)***	Performs general security services, including cryptographic operations and other approved security functions
Security Officer ***(Cryptographic Officer Role)***	Performs cryptographic initialization or management functions, such as module initialization, input/output of cryptographic keys and CSPs, and audit functions

Table 7 – ACOS5-64's Supported Roles for Operators

This cryptographic module does not allow operators to perform maintenance services thus it does not support any maintenance role.

4.2. Services

The services that can be performed by ACOS5-64 are provided by the documented APDU commands.

Services	Description	Security Officer	User
Create File	Used to create a new file under the currently selected DF or MF	Y	
Select File[2]	Used to select a file so that other operations can be performed to that file when successfully selected	Y	Y
Get Challenge[2]	Used to generate an 8-byte random challenge data for authentication purposes	Y	Y
Get Response[2]	Returns information available in the card OS, with regards to the previous command	Y	Y
Activate File	Used to activate a file so that its security settings will take effect	Y	
Deactivate File	Used to invalidate or deactivate a file so that all commands (except Activate File) to that file will be rejected	Y	
Terminate DF	Used to irreversibly send a DF to terminated state so that all commands to that file will be rejected	Y	
Terminate EF	Used to irreversibly send an EF to terminated state so that all commands to that file will be rejected	Y	

Services	Description	Security Officer	User
Delete File	Used to delete a file (except MF) and zeroizes the memory space it occupied	Y	
Security Officer File Read	Read Binary, Read Record	Y	
Security Officer Update	Update Binary, Update Record, Append Records. Update files and/or keys belonging to the security officer.	Y	
Cardholder File Read	Read Binary, Read Record		Y
Cardholder Update	Update Binary, Update Record, Append Records. Update files and/or keys belonging to the user.		Y
Erase Binary	Used to zeroize the data of a transparent file	Y	Y
Authenticate User PIN	Used to submit a User PIN to gain user access rights		Y
Logout	Used to de-authenticate the user or admin's access status	Y	Y
Change User PIN	Allows user to change the User PIN	Y	Y
Authenticate Security Officer Key	Used to submit a challenge response for Security Officer Key authentication to gain Security Officer Access Rights	Y	
Unblock User PIN	Used to reset the User Key and retry counter after being blocked	Y	
Change Security Officer Key	Allows security officer to change the Security Officer Key	Y	
Manage Security Environment (Set)[2]	Used for managing the security environment of the card. This loads initialization data in the cryptographic coprocessor RAM to prepare the use of a security operation	Y	Y
Manage Security Environment (Restore)	Used to load an existing SE record into system memory	Y	Y
Perform Security Operation	Used for security operations with regards to the ACOS5-64 cryptographic capabilities		Y
Generate RSA Key Pair	Used to generate an RSA key pair		Y
Get Card Info[2]	Used to retrieve card/file information of ACOS5-64 in the card	Y	Y
Clear Card	Clears and zeroizes all data (including Keys and CSPs) within the module and sets it back to a factory default state	Y	

[2] Unauthenticated services

Services	Description	Security Officer	User
On-Demand Self-Test[2]	Self-tests are done upon module power-up and can be used on demand by reinserting the ACOS5-64 module/card.	Y	Y

Table 8 – ACOS5-64's Available Services for Each Role

Service	Cryptographic Keys and CSPs	Type(s) of Access
Security Officer Update	Security Officer Key, Key Encryption Key	Write
Cardholder File Read	RSA Public Key	Read
Cardholder Update	RSA Private Key, AES Encryption Key, Triple-DES Encryption Key, User PIN	Write
Authenticate User PIN	User PIN	Execute
Change User PIN	User PIN	Write
Unblock User PIN	User PIN	Write
Authenticate Security Officer Key	Security Officer Key	Execute
Change Security Officer Key	Security Officer Key	Write
Perform Security Operation	RSA Private Key, RSA Public Key, AES Encryption Key, Triple-DES Encryption Key	Execute
Generate RSA Key Pair	RSA Private Key, RSA Public Key	Write
Delete File	Security Officer Key, RSA Private Key, RSA Public Key, AES Encryption Key, Triple-DES Encryption Key, User PIN	Write
Erase Binary	RSA Public Key, RSA Private Key, Certificate Files	Write
Clear Card	All Keys and CSPs	Write

Table 9 – ACOS5-64's Access Rights within Services

Services	Input	Output
Create File	File control parameters	Status word
Select File	2-byte file ID	Status word indicating length of FCI

Services	Input	Output
Get Challenge	N/A	8-byte card random challenge
Get Response	Length of data to retrieve	Card data
Activate File	2-byte file ID	Status word
Deactivate File	2-byte file ID	Status word
Terminate DF	2-byte file ID	Status word
Terminate EF	2-byte file ID	Status word
Delete File	2-byte file ID	Status word
Security Officer File Read	File record number or offset, length of data to read	Security officer file data
Security Officer Update	Security officer file data	Status word
Cardholder File Read	File record number or offset, length of data to read	User file data
Cardholder Update	User file data	Status word
Erase Binary	Offset and length of data to erase	Status word
Authenticate User PIN	User PIN	Status word (retry count on wrong PIN)
Logout	N/A	Status word
Change User PIN	Current PIN and New PIN	Status word (retry count on wrong current PIN)
Authenticate Security Officer Key	Challenge response encrypted with Security Officer Key	Status word (retry count on wrong response)
Unblock User PIN	N/A	Status word
Change Security Officer Key	New Security Officer key	Status word
Manage Security Environment (Set)	Control Reference Template	Status word
Manage Security Environment (Restore)	Security Environment record ID	Status word and Security Environment record loaded on system memory
Perform Security Operation	Cryptographic operation parameters (ciphertext/plaintext/checksum)	Status word or size of data to be retrieved by Get Response command
Generate RSA Key Pair	Key size and type	Status word and key saved in RSA key file specified by Manage Security Environment (Set)
Get Card Info	Card information type	Card information

Services	Input	Output
Clear Card	N/A	Status word
On-Demand Self-Tests	N/A	ATR with status word representing the result of the self-test

Table 10 – ACOS5-64's Service Inputs and Outputs

4.3. Authentication Mechanisms and Strength

ACOS5-64 implements identity-based authentication. A security officer and/or a user must accomplish first a challenge/response scenario using his personal key before logging in to a selected role.

The following table summarizes strength of ACOS5-64's authentication mechanism:

Role	Mechanism	Constraints	Strength of Mechanism	
			For Each Attempt*	For Multiple Attempts*
Card Holder (User)	User PIN	Any character within the Extended ASCII set (00h to FFh)	1 in 256^8	600 in 256^8 or 1 in 3.25×10^{17}
Security Officer (Cryptographic Officer - KEY)	Security Officer Key	Any character within the Extended ASCII set (00h to FFh)	1 in 256^{24}	600 in 256^{24} or 1 in 9.55×10^{56}

Table 11 – Strength of ACOS5-64's Authentication Mechanism

Security Officer can be authenticated to unblock the User key. This is done via Authenticate Security Officer Key first to gain access as the security officer role and then issue the Unblock User Key functionality for the card user.

ACOS5-64 uses an 8-byte PIN for Card Holder verification. Therefore, for each attempt to use the authentication mechanism, the probability that a random attempt will succeed in gaining unauthorized access is 1 in 256^8. This is much less than the requirement of one of 1,000,000 attempts.

ACOS5-64 uses either a 24-byte Triple-DES key, or an 8-byte PIN for Security Officer authentication. Hence, for each attempt to use the authentication mechanism, the probability is 1 in 256^8 for PIN, and 1 in 256^{24} for Triple-DES key, that a random attempt will succeed in gaining unauthorized access. This, as well, is much less than the requirement of one of 1,000,000 attempts.

For multiple attempts to use the authentication mechanism, the rate of communication dictates that each attempt will take 100ms. Therefore in a one minute period, 600 attempts can be made. The probability of a random attempt that will succeed in gaining unauthorized access will be 600 in 256^8 or 1 in 3.25×10^{17} for both the User and Cryptographic officer's PIN, and 600 in 256^{24} or 1 in 9.55×10^{56} for the Cryptographic Officer's key. This is still much less than the requirement of one out of 100,000 attempts.

The User role or the Security Officer role will be locked after reaching the maximum number of consecutive failed authentication attempts, which can be set from 1 to 15.

For both User and the Administrator role, the role authentication and identification is cleared when the device is powered off and on, reset, or if the external entity issued a Logout command.

5.0. Physical Security

ACOS5-64 module is a single-chip cryptographic module which contains a single integrated circuit. This IC is packaged directly by STMicroelectronics (the chip manufacturer) and is enclosed in a hard tamper-evident opaque epoxy which is compliant to FIPS 140-2 Level 3 Physical requirements.

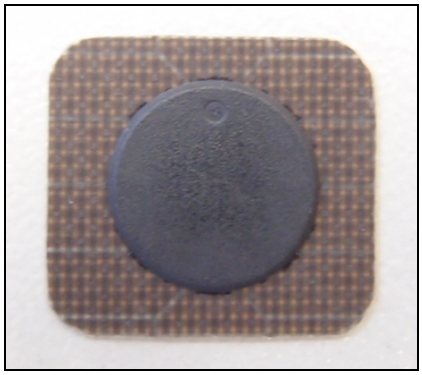

Figure 6 – ST23YL80 Physical Embodiment

The module is intended to be mounted in an external packaging, and as such, physical inspection is not practical once packaged. Physical inspection for tamper evidence is performed using a lot sampling technique during the assembly process

Any attempt at physical access or modification will leave visible signs of tamper, and has a high probability of destroying the chip which will render the plaintext secrets, private keys and CSPs inaccessible. As a result, the operator of the module is not expected to perform any periodic actions such as physical inspection in order to maintain the physical security of the module.

6.0. EMI/EMC

This cryptographic module has been tested to meet the EMI/EMC requirements specified in *FCC Part 15 Subpart B, Class B*.

7.0. Key Management

7.1. Keys and CSPs

The following table is a list of the keys and Critical Security Parameters (CSPs) that resides in ACOS5-64:

Key/CSP	File Type	Input	Output	Description	Zeroization
User PIN	8-byte PIN	Loaded at the factory and can be changed upon initialization	Never exits the module	Authenticates the User role	Clear Card, Delete File
Security Officer Key	24-byte key	Loaded at the factory and can be changed upon initialization	Never exits the module	Authenticates the SO role	Clear Card, Delete File
RSA Public Key	2048-4096 bit RSA public key with modulus	Generated onboard or externally imported in plaintext	Free to read	User public key for authentication	Clear Card, Delete File
RSA Private Key	2048-3072 bit RSA private key with modulus	Generated onboard or externally imported with encryption	Never exits the module	User private key for authentication	Clear Card, Delete File
AES Encryption Key	128/192/256-bit AES key	External import with encryption	Never exits the module	User data encryption AES key	Clear Card, Delete File
Triple-DES Encryption Key	168-bit Triple-DES key	External import with encryption	Never exits the module	User data encryption Triple-DES key	Clear Card, Delete File
Certificates	RSA signed certificate in X.501 standard	Externally loaded into the card	Free to read	User certificates for authentication	Clear Card, Delete File
K_{EK} Key Encryption Key for protecting key import	168-bit Triple-DES key	Loaded at the factory and can be re-imported in encrypted form	Never exits the module	Used to wrap keys for import	Clear Card, Delete File
DRBG V	SP800-90A DRBG internal data	Internally computed during DRBG instantiation, then subsequently updated with DRBG use	Never exits the module	Critical value of the DRBG internal state	Power Cycle
DRBG C	SP800-90A DRBG internal data	Internally computed as per SP800-90A	Never exits the module	Internal state value of the DRBG	Power Cycle

Key/CSP	File Type	Input	Output	Description	Zeroization
DRBG Entropy Input	SP800-90A DRBG internal data	Internally loaded from the module NDRNG	Never exits the module	Used to construct the seed for DRBG implementation	Power Cycle
DRBG Seed	SP800-90A DRBG internal data	Computed using SP800-90A derivation with input from NDRNG	Never exits the module	Used to determine the internal state of the DRBG	Power Cycle

Table 12 – Keys and CSPs of ACOS5-64

The private keys, secret keys and authentication keys are protected from reading from its read condition in the corresponding file set to never readable. This way, there are no commands that can access the private keys, secret keys and authentication keys that can compromise security.

To modify the public, private and encryption keys and certificates, the external entity must be authenticated to a User role. To modify the User key, the external entity must be authenticated to a User role. To modify the Security Officer key, it must be authenticated first. Without the aforementioned authentication, the CSP and keys are protected from unauthorized modifications and substitutions.

Externally imported secret keys and private keys are encrypted using 3-Key Triple-DES and authenticated using the Triple-DES MAC, which provide 112 bits of security for key wrapping.

7.2. Random Number Generators

ACOS5-64 uses a Deterministic Random Bit Generator (DRBG) based on NIST Special Publication 800-90. It uses the SHA-256 hash DRBG method.

The DRBG mechanism is seeded by an on-board Non-Deterministic Random Number Generator (NDRNG). The NDRNG is AIS-31 class P2 compliant which ensures a high level of entropy.

The module checks to ensure that two consecutively provided seeds are not identical before the later one is used as a valid input to seed the DRBG SP 800-90. The DRBG also checks that two consecutively provided seed are not identical as required by the conditional self-test.

7.3. Key Generation

The module contains RSA key generation algorithm in accordance to ANSI X9.31. The algorithm uses the DRBG to generate a set of candidate random numbers for candidate primes, in accordance to RSA algorithm. The Hash DRBG provides up to 256 bits of security, ensuring that it would take more operation to determine the seed than it would take to crack the generated RSA keys.

RSA key length in bits
2048-bits
3072-bits

Table 13 – RSA Key Length

7.4. Key Entry and Output

The *Input* and *Output* columns of **Table 12** state the key entry and output for all keys and CSPs used in ACOS5-64. Private keys and secret keys are imported into ACOS5-64 in encrypted form using Key Encryption Key (K_{EK}). The K_{EK} can itself be imported into the module by the Security Officer using secure messaging session established with the previous K_{EK}.

At the initialization at the factory, K_{EK}, initial Security Officer key, initial User key, and a PKCS#15-compliant file system is loaded in plaintext in a trusted factory into the device.

The RSA public and private key pairs can be generated on-board or loaded into the card after the User Key authentication. For the keys to be loaded, it would use the K_{EK} to encrypt the private key data before it is loaded into the card. The public key is imported in plaintext. Upon import, the keys are tested with a pair-wise consistency check to verify the validity of the keys.

Similar for secret keys, the secret keys on-board can also be loaded by the use of a K_{EK} for encryption. The function is only allowed after User Key authentication.

Authentication keys, private keys and secret keys can never be exported from the cryptographic module.

Public keys and its related CSPs (X.509 certificate) can be retrieved without the User role authentication.

The RSA public/private key pairs, and secret key files can be deleted by the Security Officer using the erase EF APDU command. These files can also be blocked by the Security Officer and key contents can also be overwritten or be zeroized by the Security Officer.

Below is a summary of the access rights of the Keys and CSPs.

Key/CSP	File Type	Update Access Rights	Key Usage Access Rights	Delete Access Rights
User PIN	8-byte PIN	User PIN / Security Officer Key	-	Security Officer Key
Security Officer Key	24-byte key	Security Officer Key	-	Security Officer Key
RSA Public Key	2048-4096 bit RSA public key with modulus	User PIN	User PIN	Security Officer Key
RSA Private Key	2048-3072 bit RSA private key with modulus	User PIN	User PIN	Security Officer Key
AES Encryption Key	128/192/256-bit AES key	User PIN	User PIN	Security Officer Key
Triple-DES Encryption Key	168-bit Triple-DES key	User PIN	User PIN	Security Officer Key
Certificates	RSA signed certificate in X.501 standard	User PIN	User PIN	Security Officer Key
K_{EK} - Key encryption Key for protecting key import	168-bit Triple-DES key	Security Officer Key	User PIN	N/A

Key/CSP	File Type	Update Access Rights	Key Usage Access Rights	Delete Access Rights
DRBG V[3]	Internal File, Store in RAM	-	-	-
DRBG C[3]	Internal File, Store in RAM	-	-	-
DRBG Entropy Input[3]	Internal File, Store in RAM	-	-	-
DRBG Seed[3]	Internal File, Store in RAM	-	-	-

Table 14 – Access Rights of ACOS5-64's Keys and CSPs

7.5. Key Storage

All the keys are stored in plaintext in the EEPROM with no access to the port and interface of the ACOS5-64 and their read/get data authorization set to *never allowed*. There is no method for retrieving the keys from the device.

[3] *These keys/CSPs are stored in the module's RAM and can be zeroized by power-cycling the module*

8.0. Self-Tests

The cryptographic module performs certain self-tests to ensure that the module is functioning properly. ACOS5-64 executes self-tests, including power-up tests at start up and conditional tests during the runtime.

The table below lists all self-tests performed by the cryptographic module:

Self-tests	Execution
Firmware Integrity Test	At power-up
Cryptographic Algorithm Test	At power-up
Random Number Generator Test	At power-up
Pair-wise Consistency Test	Conditional
Continuous DRBG Test	Conditional
Continuous NDRNG Test	Conditional

Table 15 – Self-tests Performed by ACOS5-64

8.1. Power-up Self-Test

ACOS5-64 automatically initiates power-up tests every time the module is connected to and powered by an ISO7816-compliant smart card reader.

When the power-up tests are completed, the results are to be output via the status output interface. All data output via the data output interface are inhibited while the power-up tests are being performed.

If any power-up self-test fails, the last two bytes returned by the ATR shall indicate a failure code of 66 XX where XX describes the test that failed. Upon failure and before the ATR is sent by the card, it switches into a muted state where services are no longer available.

<table>
<tr><th>Failure Code</th><th>Description</th><th>Failure Code</th><th>Description</th></tr>
<tr><td>40h</td><td>NDRNG test failed</td><td>60h</td><td rowspan="2">SHA1 test failed</td></tr>
<tr><td>41h</td><td>DRBG test failed</td><td>61h</td></tr>
<tr><td>50h</td><td rowspan="2">DES test failed</td><td>62h</td><td rowspan="2">SHA256 test failed</td></tr>
<tr><td>51h</td><td>63h</td></tr>
<tr><td>54h</td><td rowspan="3">Triple-DES test failed</td><td>70h</td><td rowspan="3">RSA test failed</td></tr>
<tr><td>55h</td><td>71h</td></tr>
<tr><td>56h</td><td>72h</td></tr>
<tr><td>58h</td><td rowspan="5">AES test failed</td><td>73h</td><td rowspan="5">Firmware integrity test failed</td></tr>
<tr><td>59h</td><td>81h</td></tr>
<tr><td>5Ah</td><td>82h</td></tr>
<tr><td>5Bh</td><td>83h</td></tr>
<tr><td>5Ch</td><td>84h</td></tr>
<tr><td>5Dh</td><td>85h</td></tr>
</table>

Table 16 – Self-tests Performed by ACOS5-64

Resetting the cryptographic module provides a means by which the operator can repeat the full sequence of power-up operating tests.

8.1.1. Firmware Integrity Test

ACOS5-64 uses firmware integrity test at start-up to ensure its firmware has not been modified. The SHA-256 hash of the module patch area is computed and compared to a known value. The test fails once the pair of values does not match.

8.1.2. Cryptographic Algorithm Test

Known Answer Tests are performed, on power-up, on the FIPS-approved algorithms indicated in **Table 17**. Triple-DES, AES and RSA algorithms are instantiated with known keys then used to perform cryptographic operations on known input data, ensuring that the produced output matches a known output. Hash algorithms follow the same process, hashing a known input then comparing the produced output to a known output.

KAT	Bit lengths
Triple-DES encryption/decryption	168
AES encryption/decryption	256
SHA-1	160
SHA-256	256
RSA signature generation/verification	2048

Table 17 – Cryptographic algorithm start-up self-test

8.1.3. Random Number Generation Test

Upon power-up, DRBG will be tested with a known answer test to ensure that any corresponding output shall match with a known input.

8.2. Conditional Self-Test

These self-tests are performed when an applicable security function or operation is invoked.

Just like in the execution of power-up tests, all data output via the data output interface are also inhibited while the conditional tests are being performed.

If any conditional tests failed, its corresponding cryptographic function shall be inhibited.

8.2.1. Pair-Wise Consistency Test

ACOS5-64 performs the pair-wise consistency test for each pair of RSA keys that it generates or imports. The consistency of the key pair is tested by calculating and verifying a digital signature within the module.

8.2.2. Conditional NDRNG Test

Every time the NDRNG is used, a continuous self-test is performed, comparing the produced random bytes with the random bytes produced through a previous call on the NDRNG. On first use, the NDRNG shall store the first 8 bytes it produces and produces a new set that shall be compared to the first 8 bytes, and then output to the user.

8.2.3. Conditional DRBG Test

Every time a DRBG is used in RSA key generation or other functions, a continuous self-test is performed in accordance to NIST SP800-90. The module generates a minimum of 8 bytes of random number per request. These 8 bytes will continuously be tested with the previous 8 bytes. If the generated data of the two requests are identical, an error state would return.

8.3. Health Tests

The DRBG performs periodic health tests to monitor and maintain assurance that it is operating as designed and implemented. Upon failure of any of the tests, any function that attempts to request a set of random bits from the DRBG shall fail.

8.3.1. Instantiate Test

Prior to creating an instantiation, the Instantiate Health Test is performed. Using fixed predetermined values, a test instantiation is created. The result is then compared to a known value, wherein a mismatch would cause the test, and the DRBG, to fail.

8.3.2. Generate and Reseed Test

On the very first use of the DRBG (the DRBG known answer test of the Power-Up Self-Test), the Reseed and Generate health test is performed, after which, will continue to be done at set intervals defined by the reseed counter. This means that every time the reseed counter of an instantiation of the DRBG reaches the defined reseed interval, the Generate and Reseed test is done using a test instantiation. Inputs for this test are fixed predetermined values and the outputs are compared to known values, wherein mismatch of which shall be considered failure of the test and the DRBG.

9.0. Mitigation of Other Attacks

ACOS5-64 module has not been designed to mitigate attacks beyond the scope of FIPS 140-2 requirements.

10.0. Security Policy Check List Tables

10.1. Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Card Holder (User)	PIN Authentication	User PIN
Administrator (Cryptographic Officer)	Key Authentication	Security Officer Key

Table 18 – Roles and Required Identification and Authentication

10.2. Strengths of Authentication Mechanism

Authentication Mechanism	Strength of Mechanism
User PIN Authentication	1~600 in 256^8
Security Officer Key Authentication	1~600 in 256^{24}

Table 19 – Strengths of Authentication Mechanism

10.3. Services Authorized for Roles

Role	Authorized Services	
Card Holder	Select File	Logout
	Get Challenge	Change User PIN
	Get Response	Manage Security Environment
	Cardholder File Read	Perform Security Operation
	Cardholder Update	Generate RSA Key Pair
	Erase Binary	Get Card Info
	Authenticate User PIN	On-Demand Self-Test
Administrator	Create File	Security Officer Update
	Select File	Manage Security Environment
	Get Challenge	Erase Binary
	Get Response	Logout
	Activate File	Authenticate Security Officer Key
	Deactivate File	Unblock User PIN
	Terminate DF	Change Security Officer Key
	Terminate EF	Get Card Info
	Delete File	Clear Card
	Security Officer File Read	On-Demand Self-Test

Table 20 – Services Authorized for Roles