Cyberflex Access 64K V2

FIPS140-2 Level 3

Cryptographic Module Security Policy

Cyberflex Access 64K V2
Cryptographic Module Security Policy

Table of Contents

Cyberflex Access 64K V2
Cryptographic Module Security Policy

1. INTRODUCTION

This document defines the Security Policy for the Cyberflex Access 64K V2 cryptographic module. The cryptographic module is an IC with its embedded firmware, designed to be put on a plastic card to produce the Cyberflex Access 64K V2 smart card as shown in figure 1.

The cryptographic module is submitted for validation, in accordance with FIPS140-2 Level 3 standard.

Included is a description of the security requirements for the Cyberflex Access 64K V2 cryptographic module and a qualitative description of how each security requirement is achieved. In particular, this security policy specifies the security rules under which the cryptographic module must operate.

Figure 1

2. OVERVIEW

The Cyberflex Access 64K V2 cryptographic module from Schlumberger contains a microprocessor and EEPROM to provide processing capability and memory for storing instructions and data. The cryptographic module loads and runs applets written in the Java programming language.

The product can be used to store and update account information, personal data, and even monetary value. The cards are ideal for secure Internet access, purchases, portable digital telephones, and for benefit programs and health care applications. Cyberflex Access 64K V2 cryptographic module brings new services, as well as increased security, portability, and convenience, to computer applications.

The Cyberflex Access 64K V2 cryptographic module combines the advantages of the Java programming language and cryptographic services with those of the micro module. Security comes from both software and hardware. Data integrity and security are provided through cryptographic services, Java Card ™ features, and the Systems Software. In addition, the Cyberflex Access 64K V2 cryptographic module hardware provides tamper-resistance and tamper-evidence features, that meet FIPS140-2 Level 3 physical requirements.

The Cyberflex Access 64K V2 cryptographic module contains an implementation of the Java Card ™ specification (JC) Version 2.1.1 and of the Open Platform (OP) Version 2.0.1' specification, which defines a secure infrastructure for post-issuance programmable smart cards. The JC specification defines Java Card ™ Application Programming Interface (API), that can be used by applets developers to take advantage of the various on-board cryptographic services. The Cyberflex Access 64K V2 cryptographic module is a "post-issuance programmable" cryptographic module. It includes a virtual machine interpreter that allows programs (applets) written in Java to be loaded onto the Cyberflex Access 64K V2 cryptographic module and placed into execution. The OP specification defines a life cycle for OP compliant smart cards. State transitions between states of the life cycle involve well-defined sequences of operations. Once applets are loaded and the Cyberflex Access 64K V2 cryptographic module is initialized, external applications communicate with Cyberflex Access 64K V2 cryptographic module through a secure channel that is established as part of the Cyberflex Access 64K V2 cryptographic module's initialization process when it is inserted into a Card Acceptance Device (CAD), or card reader. The Secure channel is established by the Cryptographic Officer with the Open Platform Card Manager application on the Cyberflex Access 64K V2 cryptographic module. Through the Card Manager, a secure communication pathway can be established with any of the applets on the Cyberflex Access 64K V2 cryptographic module. Each applet can provide additional "command services" which can be accessed by external applications.

The Cyberflex Access 64K V2 cryptographic module, validated to FIPS 140-2, is the Java Card platform, without any applet.
Applets are loaded post validation and they must also be validated to FIPS140-2 in order to keep valid the Cyberflex Access 64K V2 cryptographic module validation.
If an applet, which is not FIPS validated, is loaded on this module, the module loses its FIPS validation.

3. SECURITY LEVEL

The Cyberflex Access 64K V2 cryptographic module is designed and implemented to meet the Level 3 requirements of FIPS140-2. The cryptographic module enforces FIPS mode of operation at all times. The individual security requirements, specified for FIPS 140-2, meet the level specifications indicated in the following table.

Security Requirements Section	Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles, Services, and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self Tests	3
Design Assurance	3
Mitigation of other attacks	3

4. CRYPTOGRAPHIC MODULE SPECIFICATION

The Cyberflex Access 64K V2 cryptographic module supports a command set aimed at allowing the mutual authentication of identities using strong cryptography with “card acceptance devices” in ISO mode (and PCs or other terminals that they might be connected to). Specifically, the TDES algorithm is used within authentication commands between the cryptographic module and the “card acceptance device” environment to authenticate identities. Establishment of identities using these commands is then used to fulfill “access conditions” which limit the ability of the external world to access information and/or commands on the Cyberflex Access 64K V2 cryptographic module.

This validation effort will be aimed at the Systems software, virtual machine, and Card Manager application without any applets. If applets are added to this Cyberflex Access 64K V2 cryptographic module, then these additional applets will need to go through a separate validation and will need to be FIPS 140-2 validated. Consequently, the Cyberflex Access 64K V2 cryptographic module together with the approved applets will still be FIPS140-2 validated.

The Cyberflex Access 64K V2 cryptographic module adheres to the various ISO/IEC specifications for Integrated Circuit Chip (ICC) based identification cards. The “cryptographic boundary” for the Cyberflex Access 64K V2 cryptographic module vis-à-vis the FIPS 140-2 validation is the “module edge”. The module is comprised of the chip (ICC), the contact faceplate, and the micro-electronic connectors between the chip and contact pad.

Cyberflex Access 64K V2 cryptographic module is a single chip implementation of a cryptographic module. The Cyberflex Access 64K V2 cryptographic module chip is comprised of the following elements:

- Hardware, an IC referenced M512LACC2
- System software is installed in Read Only Memory (ROM) as part of the chip manufacturing process (known as Hard mask) and in Electrically Erasable, Programmable Read Only Memory (EEPROM) for system options and additional customized software (known as soft mask). The software is then designated by two version numbers: one for the Hard Mask and one for the Soft Mask. Note that in the smart card world, Hard Mask refers to software stored in ROM; in other guises, this might be referred to as “firmware”. These hard mask and soft mask identification numbers are returned in the response to the MaskTrack command. Three versions are available:
  - Hard Mask 1v1, Soft Mask 2v1, delivering an answer to the MaskTrack command ending by 01 01 02 01
  - Hard Mask 1v1, Soft Mask 2v3, delivering an answer to the MaskTrack command ending by 01 01 02 03
  - Hard Mask 1v2, Soft Mask 1v1, delivering an answer to the MaskTrack command ending by 01 02 01 01
- Applets that are to be loaded on Cyberflex Access 64K V2 cryptographic module (not part of the present validation),
- Critical Security Parameters stored in EEPROM as part of the Cyberflex Access 64K V2 cryptographic module personalization operation.

4.1 MODULE INTERFACES

The electrical and physical interface of the Cyberflex Access 64K V2 cryptographic module is comprised of the 8-electrical contacts from the surface of the module to the chip. These contacts conform to the following specifications.

4.1.1 Physical Interface description

The Cyberflex Access 64K V2 cryptographic module supports eight contacts that lead to pins on the chip. Only five of these are used. The location of the contacts complies with [ISO7816-2] standard. Minimum contact surface area is 1.7mm * 2.0 mm.
Contact dimensions are standard credit card compliant as per ISO/IEC 7816-1 standard:

Dimension	Value
Length	85.5mm
Width	54.0mm
Thickness	0.80mm

4.1.2 Electrical specifications

4.1.2.1 Specific electrical functions of the contacts:

Contact	Function
C1	Vcc supply voltage 3 to 5V +/- 10%
C2	RST (Reset)
C3	CLK (Clock)
C4	Reserved for Future Use (RFU)
C5	GND (Ground)
C6	Not used
C7	I/O bi-directional line
C8	Reserved for Future Use (RFU)

C4 and C8 are disabled.

4.1.2.2 ICC supply current:

Maximum value: 10 mA at 5MHz (3mA type), short time peak value according to ISO 7816-3.
The communication between the reader and the Cyberflex Access 64K V2 cryptographic module is based on a standardized, half-duplex character transmission, ISO 7816 protocol, T=0.

4.1.3 Logical Interface Description

Once electrical (physical) contact and data link layer contact is established between the module and the reader, the module functions as a “slave” processor to implement and respond to the card reader

commands. The Cyberflex Access 64K V2 cryptographic module adheres to a well-defined set of state transitions. Within each state, a specific set of commands is accessible.
The details of these commands are listed hereafter. This module also provides an additional set of internal services through the Java Card ™ APIs.

The logical interfaces are connected to the physical interfaces as follows:

Logical interface	Physical interface
Data input	C7
Data output	C7
Status output	C7
Control input	C2, C3, and C7
Power input	C1 and C5

5. ROLES & SERVICES

5.1.1 Roles

The Cyberflex Access 64K V2 cryptographic module defines two distinct roles that are supported by the internal cryptographic system: the Cryptographic Officer and the User.

- ***Cryptographic Officer***: This role is the internal security controller. The Cryptographic Officer establishes his identity on the module by demonstrating to the Card Manager application that he possesses the knowledge of a TDES key set stored within the Card Manager. By successfully executing a series of commands, the Cryptographic Officer establishes a secure channel to the Card Manager. The establishment of this channel includes mutual authentication of identities between the Cryptographic Officer and the Card Manager. Once the secure channel is established, the Card Manager grants authorization (on the module) to information and services. The Card Manager Security Domain corresponds to the Card Issuer Security Domain.
- ***User/Applet provider***: the Applet Provider is the applet developer that uses the Java API, provided on the module. He is regarded as an internal user to the module. The cryptographic services provided by the Cyberflex Access 64K V2 cryptographic module are delivered through the use of appropriate APIs. An applet has its own Security Domain (Applet Provider Security Domain).

Identity based Authentication

- ***Identification.*** The operator identifies himself by selecting his application and the key set inside the application. The application of Cryptographic Officer is the Card manager. The application of the applet provider is his own applet. The selection of the application is done by a SELECT command. The selection of the key set is done in the INITIALIZE UPDATE, the first command of the two commands that open the Secure Channel.
- ***Authentication.*** The operator authenticates himself using a mutual authentication comprising two commands INITIALIZE UPDATE and EXTERNAL AUTHENTICATION. During this mutual authentication, the operator has to encrypt a message sent by the card, proving knowledge of the TDES key set which was referenced during the identification.

Notes:

1. The CardHolder is the end user of the Cyberflex Access 64K V2 cryptographic module (when applets are loaded), who is responsible for insuring the ownership of his Cyberflex Access 64K V2 cryptographic module. The CardHolder will then be authenticated by verification of a PIN. Dedicated services are prepared on the Cyberflex Access 64K V2 cryptographic module to manage the CardHolder PIN (GlobalPIN).
2. The applets that will be downloaded onto the Cyberflex Access 64K V2 cryptographic module may define other distinct roles that will be part of the applets validation, including the Cardholder, who is responsible for insuring the ownership of his Cyberflex Access 64K V2 cryptographic module and for not communicating his PIN. The Card Holder will then be authenticated by verification of a PIN.

The Card Manager is the controlling application on the Cyberflex Access 64K V2 cryptographic module. It is invoked following every Cyberflex Access 64K V2 cryptographic module reset and initialization operation.

5.1.2 Services

5.1.2.1 Crypto Officer Administrative Services

One command set is supported by the Crypto Officer to allow for the administration of the Security Domains and to load applets onto the Cyberflex Access 64K V2 cryptographic module. This command set is used by the Crypto Officer and by Applet Providers having a Security Domain with Delegated Management privilege.

This command set includes the following commands:

- ***INSTALL (CO):*** installing an application or a Security Domain requires the invocation of several different internal functions. The INSTALL command is used to instruct the Card Manager (or a Security Domain with Delegated Management privilege) as to which installation step it shall perform during an application installation process.
- ***LOAD (CO):*** this command is used to load the byte-codes of the Load File (package) defined in the previously issued INSTALL command.
- ***DELETE (CO):*** this command is used by the Crypto Officer (or the owner of a Security Domain with Delegated Management privilege) to delete a Load File (package), an Application (applet instance) or a Security Domain.

One command is supported by the Crypto Officer to allow for the administration of the Global PIN on the module. This command is:

- **PIN CHANGE / UNBLOCK (CO)**: this command is used by the Crypto Officer to store, replace or unblock the Global PIN (Card Holder PIN).

Applets loaded onto the Cyberflex Access 64K V2 cryptographic module must be FIPS 140-2 validated.

Applets are loaded inside a Secure Channel established by the Crypto Officer with the Card Manager during the Identification/authentication process. The applet is divided in a series of blocks that fit in a LOAD command. The loading is made of a series of LOAD commands, each one transmitting a block, encrypted and followed by a TDES CBC MAC, computed with the TDES key set selected by the Crypto Officer during the identification process. The TDES CBC MAC ensures the correct transmission of each block of the applet, therefore ensuring the correct transmission of the whole applet.

Additionally (and optionally) a mechanism called “OP DAP” enables the applet provider to check, independently of the Issuer, that his applet has been correctly loaded. The applet provider can perform this check by one of the two following means:

- The “OP DAP DES” works as an EDC that verifies the integrity of the applet on behalf of the applet provider. It is made of a series of DES, ended by a TDES. All the DES and TDES operations use the applet provider ‘s keys, loaded in his Security Domain.
- The “OP DAP RSA” is a stronger mechanism. It verifies the integrity of the applet on behalf of the applet provider and it also authenticates the applet provider as the originator of the applet.

5.1.2.2 Crypto Officer & User services

Commands that are available for both the Crypto Officer & the User are the following commands:

- **SELECT**: this command is used for selecting an application (Card Manager, Security Domain or Applet). The Card Manager may be selected either for the loading of a Load File or for installing a previously loaded application (or Security Domain).
- **INITIALIZE UPDATE**: this command is used to initiate a Secure Channel with the Card Manager or a Security Domain. Cyberflex Access 64K V2 cryptographic module and host session data are exchanged, and session keys are derived in the Cyberflex Access 64K V2 cryptographic module upon completion of this command. However, the Secure Channel is not considered open until completion of a successful EXTERNAL AUTHENTICATE command that must immediately follow the INITIALIZE UPDATE command.
- **EXTERNAL AUTHENTICATE**: this command is used by the Cyberflex Access 64K V2 cryptographic module to authenticate the host, to establish the Secure Channel, and to determine the level of security required for all subsequent commands within the Secure Channel. A previous and successful execution of the INITIALIZE UPDATE command is required prior to processing this command.
- **PUT DES KEY**: this command is used to add or replace Security Domain key sets, except for the RSA DAP public key.
- **PUT RSA KEY**: this command is used to add a key set containing only the RSA DAP public key.
- **SET STATUS**: this command is used to modify the life cycle state of the Cyberflex Access 64K V2 cryptographic module or the life cycle state of an application.
- **GET STATUS**: this command is used to retrieve Card Manager information according to a given search criteria.
- **PUT DATA**: this command is used to store or replace one tagged data object provided in the command data field.
- **GET DATA**: the GET DATA command is used to retrieve a single data object. This command is available outside of a Secure Channel (no security condition). However, if issued within a Secure Channel, it must follow the same security level as defined in EXTERNAL AUTH.
- **MASK TRACK**: This command allows the reading of up to 10 traceability data bytes.
- **GET SIZE**: This command is provided to retrieve the available EEPROM memory size. It is not available on version (HM1V1, SM2V3).
- **CHANGE ATR**: This command allows modifying the ATR.
- **READ SERIAL NUMBER**: This command is provided to retrieve the chip Serial Number, which identifies the chip and therefore the cryptographic module as unique.

All commands except (Select, Initialize update, External Authentication, Get Data, Read Serial Number, and Mask Track) need a secured channel to be executed. During the secured channel opening, the command access condition is specified (’MAC’, ’MAC+ENC’) and an access control is done on received command.

5.1.2.3 Relationship between Roles & Services

Roles / Services	Crypto -Officer (Card Manager Security Domain)	User/Applet Providers (Applet Security Domain)	Unauthenticated (Any role)	Algorithms
SELECT			X	
INITIALIZE UPDATE	X	X	X	TDES, DRNG
EXTERNAL AUTHENTICATE	X	X		TDES
PUT DES KEY	X	X		TDES
PUT RSA KEY(4)	X	X		TDES
PIN CHANGE/UNBLOCK	X			TDES
INSTALL	X	X(1)		TDES
LOAD	X	X(1)		TDES, DES(3), RSA(3)
DELETE	X	X(1)		TDES
SET STATUS	X	X		TDES
GET STATUS	X	X		TDES
PUT DATA	X	X		TDES
GET DATA	X	X	X	TDES(2)
MASK TRACK	X	X	X	TDES(2)
GET SIZE	X	X		TDES(2)
CHANGE ATR	X	X		TDES
READ SERIAL NUMBER	X	X	X	TDES(2)

Table 1: Roles vs. Services

Note (1) INSTALL, LOAD & DELETE commands are available to Security Domains having the Delegated Management privilege.

Note (2) If secure messaging with MAC or MAC+ENC

Note (3) If DAP or Delegated Management

Note (4) The Put RSA Key command is only used to import the RSA Public Key used for DAP or Delegated Management

5.1.2.4 Services available for Applets

The Cyberflex Access 64k v2 Cryptographic Module implements a secure environment for execution of User-developed applications, known as Java Card Applets. Applets that are developed and downloaded onto the module shall use the Cyberflex Access 64K V2 Java APIs. These APIs are only available to applets. So they are not accessible before an applet is loaded, and are presented here as information to the User who would develop applets with the goal of obtaining a separate validation encompassing both the Cyberflex Access 64k v2 Cryptographic Module and their applets.

These APIs are listed in the CO/User guidance document. Among them, the ones that contain cryptographic services are the following:

- Key Generation:
  - RSA key pair generation: this API generates a pair of RSA keys using ANSI X9.31 approved method.
- Key Wrapping:
  - RSA algorithm API supports key wrapping/unwrapping for the key establishment. Key wrapping uses an RSA public key. Key unwrapping uses an RSA private key.
- Message Digest:
  - SHA-1: this API performs a SHA-1 Message Digest,
- Random Numbers Generation:
  - Secure Random Generation: this API generates a random data, using ANSI X9.31 FIPS140-2 approved method (Deterministic RNG).
- Signature and Verification:
  - RSA SHA-1 PKCS1 mode. Signature uses an RSA private key. Verification uses an RSA public key.
- Origin authentication and Data integrity verification:
  - TDES: these APIs offer TDES MAC in CBC mode with various padding (no padding, ISO9797 M1 and M2),
  - AES: these APIs offer AES in CBC mode with various padding (no padding, ISO9797 M1 and M2),
  - RSA SHA-1 PKCS1 mode, the RSAMAC is computed with an RSA private key. It is verified with an RSA public key
- Bulk Encryption/Decryption:
  - DES/TDES: these APIs offer DES/TDES CBC or ECB mode using various padding (no padding, ISO9797 M1 and M2),
  - AES: these APIs offer AES CBC or ECB mode using various padding (no padding, ISO9797 M1 and M2),
- PIN

  PIN APIs are available for applets to authenticate the cardholder.

These algorithms shall be used only in a FIPS approved mode of operation. This will be checked during the applet's validation. We recall that only FIPS 140-2 validated applets shall be loaded on the Cyberflex Access 64k cryptographic module.

The OP specification defines also various OP APIs that may be used by the applets and that provide the same services as the Card Manager Commands (such as secure channel opening). In particular, the Global PIN may be implemented by the applets through the use of a dedicated API.

5.1.2.5 Relationship between Roles and APIs services

All the above-mentioned applet services can be accessed by applets owned by the Card issuer or owned by another Provider. This means that these services can be related to keys stored in the Card Manager (Crypto Provider) Security Domain or in an Applet Security Domain.

5.1.2.6 Card Cryptographic Functions

The purpose of the Cyberflex Access 64K V2 cryptographic module is to provide a FIPS approved platform for applets that may in turn provide cryptographic services to end-user applications. The keys represent the identity of the roles involved in controlling the Cyberflex Access 64K V2 cryptographic module. DES, TDES, AES, RSA and SHA-1 algorithms are provided as services to applets that may be loaded onto the Cyberflex Access 64K V2 cryptographic module. These algorithms are presented via the Java Card API and shall be used only in a FIPS approved mode of operation. Validation of the use of these cryptographic services in a Java Card applet are subject to a separate validation involving the applets. This Cyberflex Access 64k v2 cryptographic module validation does not include such applets.

The Cyberflex Access 64k v2 cryptographic module cryptographic functions are as follows:

- **DES [Certificate# 227]:**
  - DES is used together with TDES as an EDC for the “OP DES DAP” and for the DM Receipt. Cf. 6.1.2.2.
  - DES functions are also provided as services to applets, through Java APIs. They shall be used only for legacy systems.
- **TDES, (2 keys TDES) [Certificate# 193]:**
  - The TDES (CBC mode) algorithm is used
    - for authenticating the Crypto Officer (EXTERNAL AUTH command)
    - for encrypting data flow from the off module to the on-module environment. The reverse direction is not encrypted; i.e. the status words returned in response to an APDU are not encrypted.
    - As a TDESMAC to authenticate the originator and to the verification the integrity of the message
  - TDES is also used together with DES as an EDC (cf. DES).
  - TDES functions are also provided as services to applets, through Java APIs.
- **AES 128 [Certificate# 81]:**
  - The AES functions are only provided as services through Java APIs to applets.
- **SHA-1 [Certificate# 173]:**
  - The SHA-1 function is only provided as a service through Java APIs to applets.
- **RSA PKCS1 (1024, 2048 bit keys) [vendor affirmed]:**
  - RSA is used for the “OP RSA DAP” as described in section 6.1.2.2.
  - RSA is used for the DM as described in section 6.1.2.3.
  - RSA functions are also provided as services to applets, through Java APIs. The applet shall use RSA only for “key wrapping” or “signature”. This will be checked during the applet’s FIPS validation.

5.1.2.7 RNG

The Cyberflex Access 64K V2 cryptographic module offers the services of a FIPS approved DRNG using ANSI X9.31 standard.

5.1.2.8 Self-Tests

5.1.2.8.1 Power Up Self Tests

The Cyberflex Access 64K V2 cryptographic module performs the required set of self-tests at power-up time. When the Cyberflex Access 64K V2 cryptographic module is inserted into a reader, once power is applied to the module' electrical (contact) interface, a "Reset" signal is sent from the reader to the module. The Cyberflex Access 64K V2 cryptographic module then performs a series of GO/NO-GO tests before it responds (as specified by ISO/IEC 7816) with an Answer To Reset (ATR) packet of information. These tests include:

- RAM functional test & clearing at Reset,
- EEPROM Firmware integrity check,
- Algorithm (known answer) tests for:
  - CRC16,
  - DES (ECB & CBC mode encrypt/decrypt),
  - TDES (ECB & CBC mode encrypt/decrypt),
  - AES (ECB & CBC mode encrypt/decrypt),
  - SHA-1 Hashing,
  - RSA PKCS1 sign and verify.
  - DRNG

If any of these tests fail, the Cyberflex Access 64K V2 cryptographic module will respond with an ATR and a status indication of self-test error. Then, the cryptographic module will go mute. No data of any type is transmitted from the cryptographic module to the reader while the self-tests are being performed.

5.1.2.8.2 Conditional Tests

RSA Key generation:

A pair wise consistency check is performed during key generation, sign and verify, encrypt and decrypt.
Note that this operation can only be activated by an applet. It is therefore out of the scope of this validation.

Random Number Generator:

NDRNG: A 16 bits continuous testing is performed during each use of the Hardware non deterministic RNG. The NDRNG is used to generate seed values to feed the DRNG.
DRNG: A 64 bits continuous testing is performed during each use of the FIPS140-2 approved deterministic RNG.

Software/Firmware load test

A TDES CBC MAC is verified whenever an applet is loaded onto the Cyberflex Access 64K V2 cryptographic module. This MAC is linked to the secure messaging
An optional DAP verification is made. The algorithm used is an RSAMAC with a public key or an algorithm using DES for the first n-1 blocks and a TDES for the last block.

5.1.3 Critical Security Parameters:

5.1.3.1 Cryptographic Keys :

The Cyberflex Access 64K V2 cryptographic module contains the following keys:

1. TDES Transport Key Set, used to protect the cryptographic module during its delivery. This Key Set will then be superseded by the Crypto Officer Security Domain keys,
2. TDES Crypto Officer Security Domain keys, used for OP authentication
3. TDES Session keys (keys derived from TDES Crypto Officer keys set(s))
4. TDES Delegated Management (DM) keys

And in addition, the key sets of each applet Security Domain.

5. TDES Applet Security Domain keys used for OP authentication
6. TDES Applet Session keys (keys derived from Applet Provider Security Domain keys set(s))
7. TDES DAP keys

The keys 1 2 & 4 are put in the Crypto-officer Security Domain key sets with the Put DES Key command.
The keys 3 & 6 are temporary keys stored in RAM.
The keys 5 & 7 are put in the Applet Security Domains key sets with the Put DES Key command.

A TDES key set contains three types of TDES keys:

- $K_{enc,auth}$ used to derive session keys for Crypto Officer authentication and encrypted mode of the secure channel,
- K_{mac}, used to derive session key for MAC mode of the secure channel,
- K_{kek} used to encrypt keys, to be imported into the platform.

For TDES DAP, only one TDES key is necessary, it is the first key of the key set.
Security Domains allow a number of distinct identities to be established on the Cyberflex Access 64K V2 cryptographic module. These are identities that control access to the various applets stored on the cryptographic module. A Security Domain represents the identity of an application (applet) operator.

5.1.3.2 Other CSPs

The Cyberflex Access 64K V2 cryptographic module includes another type of CSPs:

- A Global Personal Identification Number (PIN),

The Global PIN is 7-12 character (numeric) strings that may be used (through a dedicated OP API) to authenticate the future Cardholder to the Cyberflex Access 64K V2 cryptographic module. That is, by successfully entering a PIN sequence, a cardholder can prove knowledge of a shared secret (the PIN) and thereby authenticate to the cryptographic module.

5.1.3.3 Public Keys

The Public keys are not CSPs.

1. RSA DM key
2. RSA DAP keys

The key 1 are put in the Crypto-officer Security Domain key sets with the Put RSA Key command.
The keys 2 are put in the Applet Security Domains key sets with the Put RSA Key command.
These keys are entered only once. They cannot be updated.
DAP and DM functions are described in sections 6.1.2.2 and 6.1.2.3.

5.1.3.4 Other Cryptographic Keys

This section contains Cryptographic Keys, generated via an applet. These Keys are out of the scope of this FIPS validation because the applets that own them are also out of the scope of this validation, because this validation does not include applets.
They are mentioned here for a better understanding of the module and its limits.

1. TDES Applet Session keys (keys derived from TDES Applet Security Domain keys set(s))
2. Other keys generated or imported by the Applet for its own purposes

RSA Private keys in the Cyberflex Access 64K V2 cryptographic module belong to this category. An applet needs RSA private keys when it loads keys and uses RSA key unwrapping for this purpose.
In this case, the private key is either generated by the applet, using an API described in 5.1.2.4, or loaded by the applet with its own commands, that are not described in this document.

6. SECURITY RULES

6.1.1 Identification & Authentication Security Rules

The module implements specific methods for identifying and authenticating the different roles. The implementation consists of the binding of an Identity-based Access Control Rule to each service.

6.1.1.1 *User Identification and Authentication*

- **User/Applet Provider Authentication**: The User/Applet Provider must prove the possession of the Applet Security Domain Key Set composed of 3 TDES keys. Two keys are used to authenticate the command payload. A third key is used to encrypt keys transported within the APDU command. This is the same process as the Crypto Officer authentication (Initialize Update & External Authenticate commands) but it uses the TDES keys of the Applet Security Domains.

6.1.1.2 Cryptographic Officer Identification &Authentication

• **Crypto Officer Authentication**: The Cryptographic Officer must prove the possession of the Cyberflex Access 64K V2 cryptographic module Manager Key Set composed of 3 TDES keys. Two keys are used to authenticate the command payload. A third key is used to encrypt keys transported within the APDU command (Initialize Update & External Authenticate commands).

6.1.2 Applet Loading Security Rules

6.1.2.1 Integrity and Confidentiality of the loading

Only applets validated to FIPS 140-1 or 140-2 shall be loaded onto the Cyberflex Access 64K V2 cryptographic module.
Applets can only be loaded through a secure channel; i.e. they pass from the off module to the on-module environment in an encrypted and MACed form.
This is the only mandatory rule. It guaranties the integrity and the confidentiality of the applet during its loading. The DAP and Delegated Management features described below are considered optional but complimentary for use by the Cryptographic Officer/User and are consistent with operation of the module in FIPS mode.

6.1.2.2 Applet Loading with "OP DAP"

In this case, the Issuer (Crypto Officer) loads the applet owned by the Applet provider. The Issuer knows that the applet is correct because he loads it inside a secure channel with his own keys, thereby ensuring the applet Origin and Integrity. The Cyberflex Access 64K V2 cryptographic module provides a mechanism designated as "DAP" in OP 2.0.1' to give the same confidence to the Applet provider.

This mechanism uses a DAP, computed off-module by the Applet provider and loaded by the Issuer along with the applet. This DAP is then verified on-module with the Applet Provider 's keys, thereby ensuring that the applet loaded onto the module is the one given by the Applet Provider. The DAP verification is done systematically at the end of the loading, without any additional command.

The Cyberflex Access 64K V2 cryptographic module provides two types of DAP:

- The “OP DAP DES” works as an EDC that verifies the integrity of the applet on behalf of the applet provider. It is made of a series of DES computations, ended by a TDES computation.
  All the DES and TDES operations use the TDES DAP secret key. This TDES DAP key is loaded by the User/Applet Provider in his Security Domain, with the PUT DES KEY command. This TDES DAP key cannot be updated.
- The “OP DAP RSA” is a signature verification, which is a stronger mechanism than the “OP DAP DES”. It verifies the integrity of the applet on behalf of the applet provider and it also authenticates the applet provider as the originator of the applet. It is made of an RSA PKCS#1 (SHA-1 on the applet followed by RSA signature).
  The RSA operation uses the applet provider‘s public key. This RSA DAP key is loaded by the User/Applet Provider in his Security Domain, with the PUT RSA KEY command. This key cannot be updated.

This mechanism is optional but it is designed to be used in FIPS mode of operation.
It is described in detail in the CO / User Guidance document.

6.1.2.3 Applet Loading with Delegated Management (DM)

In this case, the Applet provider loads his own applet. The Cyberflex Access 64K V2 cryptographic module provides the Delegated Management (DM) feature as defined in [VOPS]. This feature enables the applet provider to load onto the cryptographic module an applet previously validated by the Issuer (Crypto Officer).

The DM uses two cryptographic mechanisms:

- A Token computation and verification
  A Token, also called “OP DAP RSA” is an RSAMAC computed off-module by the issuer (Crypto Officer) to allow the loading of this applet. The applet provider sends this Token along with the applet. On-module, the Card Manager verifies the token to check the Origin of the applet, (i.e. that the applet has been authorized by the Issuer) and the integrity of the applet.
  The Token verification operation uses the issuer‘s RSA DM public key. This key is loaded in the Crypto Officer Security Domain with a PUT RSA KEY command. This key cannot be updated.
- A Receipt computation and verification
  A Receipt is sent to the Issuer via the applet provider to confirm that the loading operations were done as expected. This Receipt contains data followed by an EDC. This EDC is made of a series of DES, ended by a TDES. All the DES and TDES operations use the issuer ‘s TDES DM key. This TDES DM key is loaded in the Crypto Officer Security Domain with a PUT DES KEY command. This key cannot be updated.

The DM mechanism is optional but it is designed to be used in FIPS mode of operation.
It is described in detail in the CO / User Guidance document.

6.1.3 Access Control Security Rules

- Keys must be loaded through a secure channel. Moreover, secret keys must be loaded in the encrypted form.
- Global PIN is set through a secure channel. Consequently, Global PIN is always input in the encrypted form.

6.1.4 Physical Security Rules

The physical security of the Cyberflex Access 64K V2 cryptographic module is designed to meet FIPS 140-2 level 3 requirements. A hard opaque epoxy is used to encapsulate the module to meet level 3 requirements. From the time of its manufacture, the Cyberflex Access 64K V2 cryptographic module is under the control of the cryptographic Officer until it is ultimately issued to the end user.

6.1.5 Key Management Security Policy

6.1.5.1 Cryptographic key generation

- TDES Session key derivation for Secure Channel Opening, conforming to Open Platform Card Specification v2.0.1' using FIPS140-2 approved ANSI X9.31 DRNG.

- RSA key pair generation using FIPS140-2 approved ANSI X9.31 DRNG.

6.1.5.2 Cryptographic key entry/output

Secret Keys shall always be input in encrypted format, using the Put DES Key command. In this command, the keys are encrypted using the K_{kek} Key and the TDES ECB algorithm. This command is passed within a secure channel that may be MAC+ENC. In this case the keys transferred are encrypted once again, using the session key.

6.1.5.3 Cryptographic key storage

The Keys are structured to contain the following parameters:

- Key id, which is the Id of the key,
- Algo Id, which determines which algorithm to be used,
- Integrity Mechanisms (CRC-16).

6.1.5.4 *Cryptographic key destruction*

The Cyberflex Access 64K V2 cryptographic module destroys cryptographic keys by reloading another key-set for Crypto Officer keys, Security Domains Applets Keys, or closing of secure channel for session keys**.**
Key Management Details can be found in the CO / User Guidance document.
The keys loaded for DAP and Delegated Management cannot be updated.
To delete DAP keys, the Security Domain must be deleted. This operation deletes all the keys contained in the Security Domain.
To delete DM keys, the Cryptographic Module must be put in the TERMINATED state. This operation deletes the whole EEPROM. It is enabled by the Set Status command.

6.1.6 Mitigation of attacks Security Policy

The Cyberflex Access 64K V2 cryptographic module has been designed to mitigate the following attacks:

- Timing attacks,
- Simple Power Analysis,
- Differential Power Analysis.
- Differential Fault Analysis

7. SECURITY POLICY CHECK LIST TABLES

7.1 ROLES & REQUIRED AUTHENTICATION

Role	Type of authentication	Authentication data
Crypto Officer	TDES authentication	TDES keys (Crypto Officer Security Domain)
User/Applet Provider	TDES authentication	TDES keys (Applet Security Domain)

7.2 STRENGTH OF AUTHENTICATION MECHANISMS

Authentication Mechanism	Strength of Mechanism
TDES authentication	Probability that a random attempt succeeds is less than 1 in 1,000,000
RSA authentication	Probability that a random attempt succeeds is less than 1 in 1,000,000

7.3 SERVICES AUTHORIZED FOR ROLES

Role	Authorized Services
Crypto Officer	CO Administrative Services as listed in Section 5.1.2.1 CO & User Services as listed in Section 5.1.2.2
User/Applet Provider	CO & User Services as listed in Section 5.1.2.2. APIs as listed in Section 5.1.2.4.

7.4 ACCESS RIGHTS WITHIN SERVICES

CSP	Service	Role	Types of Access
TDES CO Master Keys	PUT DES KEY command	Crypto Officer	Write
TDES CO Master Keys	INITIALIZE UPDATE & EXTERNAL AUTH	Crypto Officer	Execute
TDES CO Master Key: K_{KEK}	PUT KEY command (encryption of the key)	Crypto Officer	Execute
TDES CO Session Keys	INITIALIZE UPDATE & EXTERNAL AUTH	Crypto Officer	Create
TDES CO Session Key: K_{enc}	Message encryption	Crypto Officer	Execute
TDES CO Session Key: K_{mac}	Message integrity	Crypto Officer	Execute
TDES CO DM Key	PUT DES KEY command	Crypto Officer	Write
TDES CO DM Key	DM Receipt computation	Crypto Officer	Execute
TDES User Master Keys	PUT KEY command	User	Write
TDES User Master Keys	INITIALIZE UPDATE & EXTERNAL AUTH	User	Execute
TDES User Master Key: K_{KEK}	PUT KEY command (encryption of the key)	User	Execute
TDES User Session Keys	INITIALIZE UPDATE & EXTERNAL AUTH	User	Create
TDES User Session Key: K_{enc}	Message encryption	User	Execute
TDES User Session Key: K_{mac}	Message integrity	User	Execute
TDES User “OP DAP DES” Key	PUT DES KEY command	User	Write
TDES User “OP DAP DES” Key	“OP DAP” verification	User	Execute
Global PIN	PIN CHANGE command	User	Write

Public Keys	Service	Role	Types of Access
RSA CO DM Public Key	PUT RSA KEY command	Crypto Officer	Write
RSA CO DM Public Key	DM DAP verification	Crypto Officer	Execute
RSA User “OP DAP RSA” Public Key	PUT RSA KEY command	User	Write
RSA User “OP DAP RSA” Public Key	“OP DAP” verification	User	Execute

7.5 MITIGATION OF OTHER ATTACKS

Other Attacks	Mitigation Mechanism	Specific Limitations
Timing attacks	Counter Measures against Timing attacks	N/A
Simple Power Analysis	Counter Measures against SPA	N/A
Differential Power Analysis	Counter Measures against DPA	N/A
Differential Fault Analysis	Counter Measures against DFA	N/A

8. REFERENCES

Reference	Title
[JVM]	Java Card ™ 2.1.1 Virtual Machine Specification, Sun Microsystems
[JCAPI]	Java Card ™ 2.1.1 Application Programming Interface, Sun Microsystems
[JCDG]	Java Card ™applet developer's guide
[JCRE]	Java Card ™ 2.1.1 Runtime Environment (JCRE) Specification, Sun Microsystems
[VOPS]	Open Platform Card Specification, v2.0.1', Visa International
[VOPI]	Visa Open Platform Card Implementation Specification - march 1999, Visa International
[ISO7816-1]	ISO/IEC JTC 1/SC 17/WG4 Integrated circuits() cards with contacts – Part 1: Physical Characteristics
[ISO7816-2]	ISO/IEC JTC 1/SC 17/WG4 Integrated circuits() cards with contacts – Part 2: Dimension and Location of the contacts
[ISO7816-3]	ISO/IEC JTC 1/SC 17/WG4 Integrated circuits() cards with contacts – Part 3: Electronic signals and transmission protocol
[X9.31]	American Bankers Association, Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), ANSI X9.31-1998, Washington, D.C., 1998.
[FIPS140-2]	National Institute of Standards and Technology, FIPS 140-2 standard.
[FIPS140-2A]	National Institute of Standards and Technology, FIPS 140-2 Annex A: Approved Security Functions.
[FIPS140-2B]	National Institute of Standards and Technology, FIPS 140-2 Annex B: Approved Protection Profiles,
[FIPS140-2C]	National Institute of Standards and Technology, FIPS 140-2 Annex C: Approved Random Number Generators
[FIPS140-2D]	National Institute of Standards and Technology, FIPS 140-2 Annex D: Approved Key Establishment Techniques
[DES]	National Institute of Standards and Technology, Data Encryption Standard, Federal Information Processing Standards Publication 46-3, October 25, 1999.
[DES Modes]	National Institute of Standards and Technology, DES Modes of Operation, Federal Information Processing Standards Publication 81, December 2, 1980.

9. ACRONYMS

Acronyms	Definitions
AES	Advanced Encryption Standard
ANSI	Americain National Standards Institute
AP	Application Provider
API	Application Programming Interface
ATR	Answer To Reset
CAD	Card Acceptance Device
CBC	Cipher Block Chaining
CO	Crypto Officer
CRC	Cycling Redundancy Check
DAP	Data Authentication Pattern
DES	Data Encryption Standard
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
DM	Delegated Management
DRNG	Deterministic Random Number Generator
ECB	Electronic Code Book
EEPROM	Electrically Erasable and Programmable Read Only Memory
EMI	Electromagnetic Interference
EMC	Electromagnetic Compatibility
ICC	Integrated Circuit Card
ISO	International Organization for Standardization
JC	Java Card ™
JCRE	Java Card ™ Runtime Environment
MAC	Message Authentication Code
NDRNG	Non Deterministic Random Number Generator
OP	Open Platform
PC	Personnal Computer
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standards
PRNG	Pseudo Random Number Generator
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read only Memory
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SPA	Simple Power Analysis
TDES	Triple DES