Cyberflex Access 64K

FIPS140-2 Level 3

Cryptographic Module Security Policy

Table of Contents

1. INTRODUCTION

This document defines the Security Policy for the Cyberflex Access 64K 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 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 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 cryptographic module from Axalto 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 cryptographic module brings new services, as well as increased security, portability, and convenience, to computer applications.

The Cyberflex Access 64K cryptographic module combines the advantages of the Java programming language and cryptographic services with those of the micro module. Cyberflex Access 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 module hardware provides tamper-resistance and tamper-evidence features, that meet FIPS140-2 Level 3 physical requirements.

The Cyberflex Access 64K 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 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 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 module is initialized, external applications communicate with Cyberflex Access 64K through a secure channel that is established as part of the Cyberflex Access 64K 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 module. Through the Card Manager, a secure communication pathway can be

established with any of the applets on the Cyberflex Access 64K module. Each applet can provide additional “command services” which can be accessed by external applications.

Applets loaded post validation must also be validated to FIPS140-2 in order to keep valid the Cyberflex Access 64K cryptographic module validation.

3. SECURITY LEVEL

The Cyberflex Access 64K cryptographic module is designed and implemented to meet the Level 3 requirements of FIPS140-2. The cryptographic module enforces FIPS mode of operation at any time. 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 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 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 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 cryptographic module together with the approved applets will still be FIPS140-2 validated.

Cyberflex Access 64K module adheres to the various ISO/IEC specifications for Integrated Circuit Chip (ICC) based identification cards. The “cryptographic boundary” for the Cyberflex Access 64K 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 is a single chip implementation of a cryptographic module. The Cyberflex Access 64K chip is comprised of the following elements:

- Hardware, an IC referenced M512LACC1

- 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 Answer To Reset (ATR) character string following the issuing of a RESET signal to the Cyberflex Access 64K module. Three versions are available:
  Hard Mask n°5 Version 01, Soft Mask n°2 Version 01, delivering an ATR ending by 05 01 02 01.
  Hard Mask n°5 Version 01, Soft Mask n°4 Version 01, delivering an ATR ending by 05 01 04 01.
  Hard Mask n°5 Version 01, Soft Mask n°4 Version 02, delivering an ATR ending by 05 01 04 01 and delivering an answer to the Mask Track command ending by 05 01 04 02.
  The second differs from the first only by a functional bug fix.
- Applets that are to be loaded on Cyberflex Access 64K module (not part of the present validation),
- Critical Security Parameters stored in EEPROM as part of the Cyberflex Access 64K module personalization operation.

4.1 MODULE INTERFACES

The electrical and physical interface of the 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 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 ISO/IEC 7816-2 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 +/- 0.5V
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)

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 card reader and the Cyberflex Access 64K cryptographic module is based on a standardized, half-duplex character transmission, ISO 7816 protocol.

Both protocols T=0 and T=1 are supported.

4.1.3 Logical Interface Description

Once electrical (physical) contact and data link layer contact is established between the Cyberflex Access 64K module and the card reader, the Cyberflex Access 64K module functions as a “slave” processor to implement and respond to the card reader commands. The Cyberflex Access 64K 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 Cyberflex Access 64K module also provides an additional set of on-module services through the Java Card ™ APIs. These additional services are described in section 5.1.2.4.

5. ROLES & SERVICES

5.1.1 Roles

The Cyberflex Access 64K 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 on module security controller. The Cryptographic Officer establishes his identity on the Cyberflex Access 64K 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; establishment of this channel includes mutual authentication of identities between the Cryptographic Officer and the Card Manager. Once established, authorization (on the Cyberflex Access 64K module) to information and services is granted by the Card Manager. 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 Cyberflex Access 64K module. He is regarded as an internal user to the Card. The cryptographic services provided by the Cyberflex Access 64K 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 module (when applets are loaded), who is responsible for insuring the ownership of his Cyberflex Access 64K module. The CardHolder will then be authenticated by verification of a PIN. Dedicated services are prepared on the Cyberflex Access 64K module to manage the CardHolder PIN (GlobalPIN).
2. The applets that will be downloaded onto the Cyberflex Access 64K 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 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 module. It is invoked following every Cyberflex Access 64K 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, and is, in fact, used only by the Crypto Officer to allow for the administration of the Security Domains and to load applets onto the Cyberflex Access 64K module. This command set includes the following commands:

- ***INSTALL (CO):*** installing an application or a Security Domain requires the invocation of several different on-module functions. The INSTALL command is used to instruct a Security Domain or the Card Manager 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 to delete a Load File (package) or an Application (applet instance).
- **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 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 TDESMAC with the TDES key set selected by the Crypto Officer during the identification process. The TDESMAC 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. This check is done by an EDC on the applet. This EDC is a TDES CBC MAC, using the applet provider‘s keys, loaded in his Security Domain.

5.1.2.2 Crypto Officer & User services

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

- **EXTERNAL AUTHENTICATE**: this command is used by the Cyberflex Access 64K 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.
- **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.
- **GET STATUS**: if the Card Manager is the current application, this command is used to retrieve Card Manager information according to a given search criteria.

- **GET RESPONSE**: this command is restricted to T = 0 ISO protocol for an incoming command which have data to send back. That data is received with the GET RESPONSE command sent immediately after the command it is related to.
- **INITIALIZE UPDATE**: this command is used to initiate a Secure Channel with the Card Manager or a Security Domain. Cyberflex Access 64K module and host session data are exchanged, and session keys are generated by the Cyberflex Access 64K 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.
- **PUT DATA**: this command is used to store or replace one tagged data object provided in the command data field.
- **PUT KEY**: this command is used to add or replace Security Domain key sets.
- **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).
- **PRNG Statistical Test**: this command is used to execute the FIPS140-2 approved statistical tests for randomness on the PRNG.
- **SET STATUS (CO & User)**: this command is used to modify the life cycle state of the Cyberflex Access 64K module or the life cycle state of an application.
- **GET SIZE**: This command is provided to retrieve the available EEPROM memory size. It is not available on version (HM5V1, SM2V1).
- **MASK TRACK**: This command allows the reading of up to 10 traceability data bytes. It is not available on versions (HM5V1, SM2V1) and (HM5V1, SM4V1).

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

5.1.2.3 Relationship between Roles & Services

Roles/Services	Crypto -Officer (Card Manager Security Domain)	User/Applet Providers (Applet Provider Security Domain)	Unauthenticated (Any role)
INSTALL	X		
LOAD	X		
DELETE	X		
EXTERNAL AUTHENTICATE	X	X	
GET DATA			X
GET STATUS			X
GET RESPONSE			X
INITIALISE UPDATE	X	X	
PIN CHANGE/UNBLOCK	X		
PUT DATA	X	X	
PUT KEY	X	X	
SELECT			X
PRNG Statistical TEST	X	X	X
SET STATUS	X	X	
GET SIZE	X	X	
MASK TRACK	X	X	X

5.1.2.4 Applets Services

Applets that are developed and downloaded onto the Cyberflex Access 64K module shall use the Cyberflex Access 64K Java APIs. These APIs are listed in the product technical specifications detailed as a separate proprietary document. Among them, the ones that contain cryptographic services are the following:

- Key Generation/Exchange:
  - RSA key pair generation: this API generates a pair of RSA keys using ANSI X9.31 approved method.
  - Key exchange: RSA algorithm API supports key wrapping/unwrapping.
- 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.
- Origin authentication and Data integrity verification:
  - DES/TDES: these APIs offer DES or TDES MAC in CBC mode with various padding (no padding, ISO9797 M1 and M2).
- Bulk Encryption/Decryption:

- DES/TDES: these APIs offer DES/TDES CBC or ECB mode using various padding (no padding, ISO9797 M1 and M2).

These algorithms shall be use only in a FIPS approved mode of operation. This will be checked during the applet's validation.
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

Roles/Services	Crypto-Officer (Card Manager Security Domain)	Applet Providers/User (Applet Provider Security Domain)
RSA Key generation	X	X
SHA-1	X	X
Secure Random Generation	X	X
DES/TDES MAC Signature and Verification	X	X
RSA SHA-1 PKCS1 Signature and Verification	X	X
DES/TDES Encryption/Decryption	X	X
RSA PKCS1 Key wrapping	X	X

The APIs are dedicated to applets. The Crypto-Officer can use these APIs if he owns an applet and only through this applet.

5.1.2.6 Card Cryptographic Functions

The purpose of the 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 module. A variety of FIPS 140-2 validated algorithms are used in the Cyberflex Access 64K cryptographic module to provide cryptographic services; these include:

- **DES [Cert.# 179]**:
  - DES functions are provided as services to applets, through Java APIs. They shall be used only for legacy systems.
- **TDES, (2 keys TDES) [Cert.# 125]**:
  - 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 as an EDC to enable the Applet Provider to verify the correct loading of the applet.
  - TDES functions are also provided as services to applets, through Java APIs.
- **SHA-1 [Cert.# 108]**:
  - The SHA-1 function is only provided as a service through Java APIs to applets.

- **RSA PKCS1 (512, 768, 1024 bit keys) [Cert.# 58]**:
  - RSA functions are only 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.

DES, TDES, RSA and SHA-1 algorithms are provided as services to applets that may be loaded onto the Access 64K module. These algorithms shall be use only in a FIPS approved mode of operation. This will be checked during the applet’s validation.

5.1.2.7 RNG

The cryptographic module offers the services of a FIPS approved PDRNG using ANSI X9.31 standard.

5.1.2.8 Self Tests

5.1.2.8.1 Power Up Self Tests

The Cyberflex Access 64K cryptographic module performs the required set of self-tests at power-up time. When the Cyberflex Access 64K module is inserted into a reader, once power is applied to the module’s electrical (contact) interface, a “Reset” signal is sent from the reader to the Cyberflex Access 64K module. The Cyberflex Access 64K 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,
- HRNG functional test,
- EEPROM Firmware integrity check,
- Algorithm (known answer) tests for:
  - CRC16,
  - DES (ECB & CBC mode encrypt/decrypt),
  - TDES (ECB & CBC mode encrypt/decrypt),
  - SHA-1 Hashing,
  - RSA PKCS1 sign and verify,
  - DRNG.

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

Random Number Generator:

HRNG: A 16 bits continuous testing is performed during each use of the Hardware non deterministic RNG. The HRNG is used to generate seed values to feed the PRNG.

PRNG: A 16 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 each time an applet is loaded onto the Cyberflex Access 64K module.

An optional “OP DAP” verification is made. This is an EDC that enables the Applet Provider Security Domain to check that the applet has been correctly loaded. The algorithm used is TDES CBC MAC.

5.1.3 Critical Security Parameters:

5.1.3.1 Cryptographic Keys :

The Cyberflex Access 64K cryptographic module includes the following keys:
1. Initialization Key, K_{init} used only for the first Card Manager key-set loading,
2. Crypto Officer (Card Manager) Security Domain keys,
3. TDES Session keys (keys derived from Crypto Officer keys set(s))

And in addition, applets Security Domain keys sets.
4. TDES Applet Provider Security Domain keys used for OP authentication
5. TDES Applet Session keys (keys derived from Applet Provider Security Domain keys set(s))
6. "OP DAP" TDES key. This key is used as an EDC that enables the applet provider to check, independently of the Issuer, that his applet has been correctly loaded.

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

A Security Domain key set is structured in such a way as to contain 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 DAP, only one 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 module. These are identities that control access to the various applets stored on the Cyberflex Access 64K module. A Security Domain represents the identity of an application (applet) operator.

5.1.3.2 Other CSPs

The Cyberflex Access 64K cryptographic module includes another type of CSP:
- 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 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 Cyberflex Access 64K module. There is a general-purpose command supported by the Crypto Officer to change or unblock a PIN, but there is no general command to verify a PIN. A "verify PIN" command is provided by the applets through the use of APIs.

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 Key Set composed of 3 TDES keys. Two keys are used to encrypt, authenticate and check the integrity of the command data. 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 Provider Security Domains.

6.1.1.2 Cryptographic Officer Identification &Authentication

- **Crypto Officer Authentication**: The Cryptographic Officer must prove the possession of the Card Manager Key Set composed of 3 TDES keys. Two keys are used to encrypt, authenticate and check the integrity of the command data. A third key is used to encrypt keys transported within the APDU command. This is the same process as the User authentication (Initialize Update & External Authenticate commands).

6.1.2 Applet Loading Security Rules

Only applets validated to FIPS 140-1 or 140-2 shall be loaded onto the Cyberflex Access 64K 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.

6.1.2.1 "OP DAP"

In the Cyberflex Access 64K module, the applet is always loaded by the Issuer (Cryptographic Officer). The optional mechanism designated as "DAP" in OP 2.0.1' enables the applet provider to check, independently of the Issuer (Cryptographic Officer), that his applet has been correctly loaded. This check is done by an EDC on the applet. This EDC uses the TDES CBC MAC algorithm. All the TDES operations use an applet provider's TDES key, loaded in his Security Domain.
This process 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. Consequently, keys are always 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 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. Once it is manufactured, the Cyberflex Access 64K module belongs to 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 PRNG.

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

6.1.5.2 Cryptographic key entry/output

Keys shall always be input in encrypted format, using the Put Key command within a secure channel. During this process, the keys are double encrypted (using the Session Key and the K_{kek} 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.

6.1.5.4 *Cryptographic key destruction*

The Cyberflex Access 64K 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 a specific proprietary document.
The keys loaded for “OP DAP” cannot be updated. To delete an “OP DAP” key, the Security Domain containing the key must be deleted. This operation deletes all the keys contained in the Security Domain.

6.1.6 Mitigation of attacks Security Policy

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

- Simple Power Analysis,
- Differential Power 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 Provider Security Domain)

7.2 STRENGTH OF AUTHENTICATION MECHANISMS

Authentication Mechanism	Strength of Mechanism
TDES authentication	High

7.3 SERVICES AUTHORIZED FOR ROLES

Role	Authorized Services
Crypto Officer	All CO Services as listed in Section 5.1.2.2. The CO can also access all APIs, as listed in Section 5.1.2.4 if he owns an applet and only through this applet.
User/Applet Provider	Only CO Services as listed in Section 5.1.2.2 and all 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 KEY command	Crypto Officer	Write
TDES CO Master Keys	INITIALIZE UPDATE & EXTERNAL AUTH	Crypto Officer	Read & Execute
TDES CO Master Key: K_{KEK}	PUT KEY command (encryption of the loaded Key)	Crypto Officer	Read & Execute
TDES CO Session Keys	INITIALIZE UPDATE & EXTERNAL AUTH	Crypto Officer	Create
TDES CO Session Key: K_{enc}	Message encryption	Crypto Officer	Read & Execute
TDES CO Session Key: K_{mac}	Message integrity	Crypto Officer	Read & Execute
TDES User Master Keys	PUT KEY command	User	Write
TDES User Master Keys	INITIALIZE UPDATE & EXTERNAL AUTH	User	Read & Execute
TDES User Master Key: K_{KEK}	Key encryption (when loading a key)	User	Read & Execute
TDES User Session Keys	INITIALIZE UPDATE & EXTERNAL AUTH	User	Create
TDES User Session Key: K_{enc}	Message encryption	User	Read & Execute
TDES User Session Key: K_{mac}	Message integrity	User	Read & Execute
“OP DAP” TDES Key	PUT KEY command	User	Write
“OP DAP” TDES Key	EDC by Applet Provider Security Domain	User	Read & Execute
Global PIN	PIN CHANGE command	Crypto Officer	Write

7.5 MITIGATION OF OTHER ATTACKS

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

8. REFERENCES

[JVM] Java Card ™ 2.1 Virtual Machine Specification v1.1 - june 1999, Sun Microsystems
[JCAPI] Java Card ™ 2.1 Application Programming Interface, Sun Microsystems
[JCDG] Java Card ™applet developer's guide
[JCRE] Java Card ™ 2.1 Runtime Environment (JCRE) Specification, Sun Microsystems
[VOPS] Open Platform Card Specification, v2.0.1' - april 2000
[VOPI] Visa Open Platform Card Implementation Specification - march 1999, Visa International
[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.
[DSS] National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2, January 27, 2000.

9. ACRONYMS

Acronyms	Definitions
AP	Application Provider
ATR	Answer To Reset
API	Application Programming Interface
CBC	Cipher Block Chaining
DAP	Data Authentication Pattern
DES	Data Encryption Standard
ECB	Electronic Code Book
EEPROM	Electrically Erasable and Programmable Read Only Memory
JCRE	Java Card ™ Runtime Environment
MAC	Message Authentication Code
OP	Open Platform
PIN	Personal Identification Number
RAM	Random Access Memory
ROM	Read only Memory