Cyberflex Access E-gate V3

FIPS 140-2 Level 3

Cryptographic Module Security Policy

Cyberflex Access E-gate V3
Cryptographic Module Security Policy

Table of Contents

1. INTRODUCTION

This document defines the Security Policy for the Cyberflex Access E-gate V3 cryptographic module. This single-chip cryptographic module is composed mostly of a silicon chip containing a microprocessor, a crypto-processor, and an operating system burned in Read Only Memory (ROM), designed to be embedded on a plastic card to produce the Cyberflex Access E-gate V3 smart card, as shown in Figure 1.

Figure 1 – Example of Smart Card

The cryptographic module is submitted for validation, in accordance with FIPS 140-2 Level 3 standard.

Included are a description of the security requirements for the Cyberflex Access E-gate V3 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.

2. OVERVIEW

The Cyberflex Access E-gate V3 cryptographic module (HW P/N A1002431, Version A.12; FW Versions: HardMask 3v1, SoftMask 1v1) from Gemalto is a single chip module that contains a microprocessor, a crypto-processor and memory to provide secure storage for critical information and custom programs, and processing capabilities to interact with these elements. This module is compliant with JavaCard™ specification, which enables issuers to load and run their own processes, called applets, written in Java programming language.

This product can be used to manage keys and passwords, to store and update account information, personal data, and also control debit/credit operations. Smart card deployment covers a wide range of applications such as Internet security, Banking, mobile telecommunication, loyalty and health care. The Cyberflex Access E-gate V3 cryptographic module brings new services, as well as increased security, portability, and convenience, to computer applications.

The Cyberflex Access E-gate V3 cryptographic module combines the advantages of Java programming language with the ones of the cryptographic features provided by micro modules. Security comes from both software and hardware. Data security and process integrity are provided thanks to JavaCard™ features of the operating system. In addition, Cyberflex Access E-gate V3 cryptographic module hardware provides tamper-resistance and tamper-evidence features, that meet FIPS140-2 Level 3 physical requirements.

The Cyberflex Access E-gate V3 cryptographic module is compliant with JavaCard™ specification (JC) Version 2.2.1 and Global Platform specification (GP) Version 2.1.1 [GP211], which define a secure infrastructure for post-issuance programmable smart cards. JavaCard™ specification defines JavaCard ™ Application Programming Interface (API) that can be used by application developers to take advantage of the various on-board cryptographic services. It also defines a virtual machine interpreter and execution context that allow applications (applets) written in Java to be loaded onto the Cyberflex Access E-gate V3 cryptographic module and placed into execution. Global Platform specification defines a life cycle for programmable smart cards to enable post-issuance features. Transitions between each stage of this life cycle involve well-defined sequences of operations.

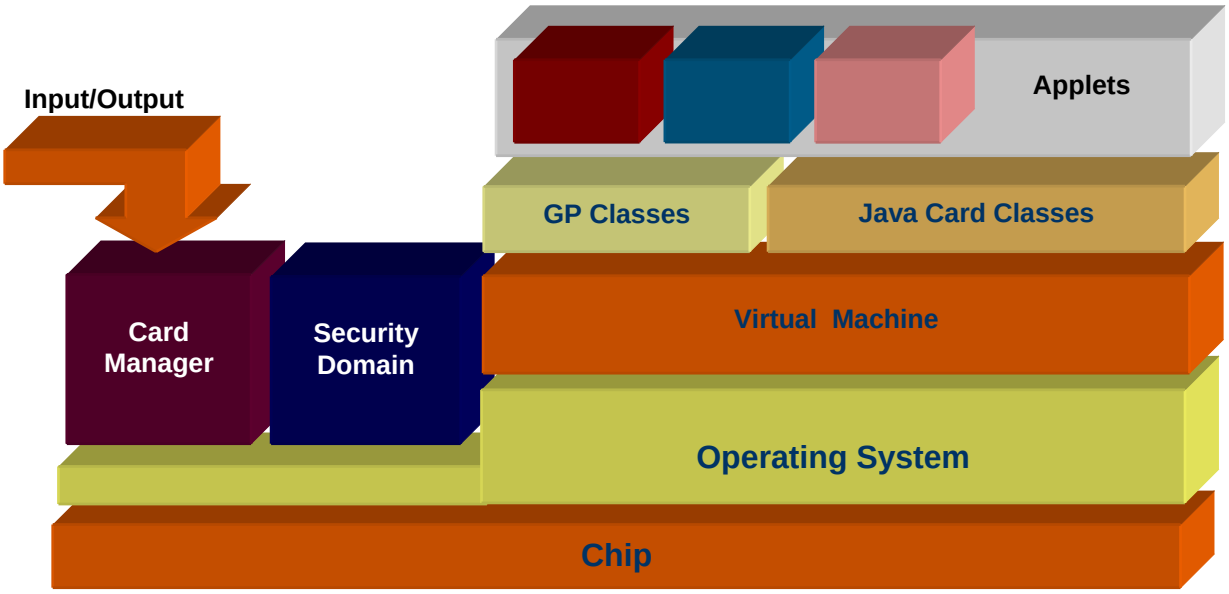


Figure 1 Internal Infrastructure

Once the Cyberflex Access E-gate V3 cryptographic module is initialized, the Card Manager controls Input and Output. Card issuers can open secure channels to authenticate themselves and communicate securely with the card to load applets and exchange information when the card is inserted into a Card Acceptance Device (CAD), or card reader. Each applet can provide custom commands, which can be accessed by external applications to deliver specific services.

The Cyberflex Access E-gate V3 cryptographic module, validated to FIPS 140-2 Level 3, is the Java Card platform, without any applet.

Applets that are loaded after validation must also be validated to FIPS 140-2 in order to make the validation for the overall product applicable.

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 E-gate V3 cryptographic module is designed and implemented to meet the Level 3 requirements of FIPS 140-2. 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 E-gate V3 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 E-gate V3 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 E-gate V3 cryptographic module, then these additional applets will need to go through a separate FIPS 140-2 validation. Consequently, the Cyberflex Access E-gate V3 cryptographic module together with the Approved applets will still be FIPS 140-2 validated.

The Cyberflex Access E-gate V3 cryptographic module adheres to the various ISO/IEC specifications for Integrated Circuit Chip (ICC) based identification cards. The “cryptographic boundary” for the Cyberflex Access E-gate V3 cryptographic module vis-à-vis the FIPS 140-2 validation is the “module edge”. The module is comprised of the chip (ICC), the hard opaque epoxy, the contact faceplate, and the micro-electronic connectors between the chip and contact pad.

4.1 MODULE IDENTIFICATION

The Cyberflex Access E-gate V3 cryptographic module is a single chip implementation of a cryptographic module. The Cyberflex Access E-gate V3 cryptographic module chip is comprised of the following elements:

- Hardware, an IC referenced A1002431
- 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). Two version numbers identify the software: one for the Hard Mask (HM) and one for the Soft Mask (SM). 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. One version is available:
  - Hard Mask 3v1, Soft Mask 1v1, delivering an answer to the MaskTrack command containing 03 01 01 01
- Applets that are to be loaded on Cyberflex Access E-gate V3 cryptographic module (not part of the present validation)
- Critical Security Parameters stored in EEPROM as part of the Cyberflex Access E-gate V3 cryptographic module personalization operation.

4.2 MODULE INTERFACES

The Cyberflex Access E-gate V3 cryptographic module supports two protocols: ISO 7816-3 T=0 protocol and USB low speed protocol. T=0 protocol requires a card reader while USB requires a USB connector. At reset time, the card detects the connection and chooses its protocol accordingly.

The electrical and physical interface of the Cyberflex Access E-gate V3 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.

4.2.1 Physical Interface description

The Cyberflex Access E-gate V3 cryptographic module supports eight contacts that lead to pins on the chip. Only seven of these are used. The location of the contacts complies with [ISO7816-2] standard. Minimum contact surface area is 1.7mm * 2.0 mm.

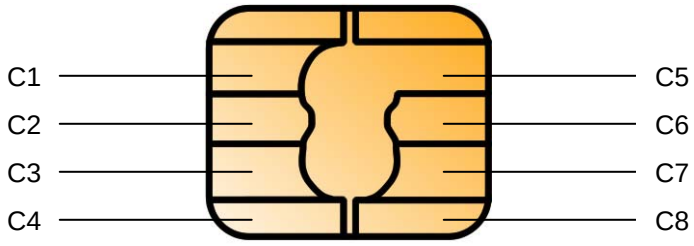


Figure 2 Design of Contact Interface

Contact dimensions are compliant to [ISO 7816-1].

Electrical features of the card are described in [ISO 7816-3].

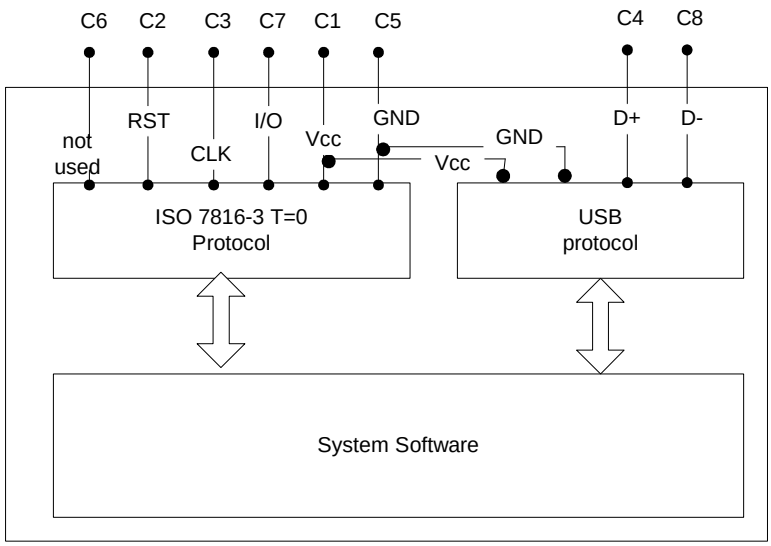
Dimension	Value
Length	85.5mm
Width	54.0mm
Thickness	0.80mm

4.2.2 Electrical specifications

4.2.2.1 Specific electrical functions of the contacts:

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

Note: C6 is not connected.



4.2.2.2 ICC supply current:

Maximum value: 10 mA at 5MHz (3mA type), short time peak value according to ISO 7816-3. Communication between the reader and the Cyberflex Access E-gate V3 cryptographic module is based on a standardized, serial, half-duplex character transmission, ISO 7816 protocol, T=0 and USB.

4.2.3 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 card reader commands. The Cyberflex Access E-gate V3 cryptographic module adheres to a well-defined set of state transitions. Within each state, a specific set of commands is accessible. 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**	
	ISO mode	**USB mode**
Data input	C7	C4 and C8
Data output	C7	C4 and C8
Status output	C7	C4 and C8
Control input	C2, C3, and C7	C4 and C8
Power input	C1 and C5	C1 and C5

Note: C6 is not connected.

5. ROLES & SERVICES

5.1 ROLES

The Cyberflex Access E-gate V3 cryptographic module defines two distinct roles that are supported by the internal cryptographic system: the Cryptographic Officer and the User/Applet Provider.

- ***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 a secure channel is established, the Card Manager grants authorization (on the module) to information and services. The Card Manager Security Domain corresponds to Card Issuer Security Domain.

- ***User/Applet Provider***: The Applet Provider is the applet developer that uses Java API, provided by the module. Cryptographic services provided by the Cyberflex Access E-gate V3 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 the application appropriate for his role and the key set inside the application. The application of Cryptographic Officer is the Card Manager. The application of the User/Applet Provider is his own applet. Selection of the application is done by a SELECT command. Selection of the key set is done in the INITIALIZE UPDATE command, the first command of the two commands to open a 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 E-gate V3 cryptographic module (when applets are loaded), who is in charge of insuring the ownership of his Cyberflex Access E-gate V3 cryptographic module...
2. Applets that will be downloaded onto the Cyberflex Access E-gate V3 cryptographic module may define other distinct roles that will be part of the applet's validation.

The Card Manager is the controlling application on the Cyberflex Access E-gate V3 cryptographic module. It is invoked following every Cyberflex Access E-gate V3 cryptographic module reset and initialization operation.

5.2 SERVICES

5.2.1 Crypto Officer Administrative Services

A set of commands is provided to the Crypto Officer for Security Domain administration and applet loading onto the Cyberflex Access E-gate V3 cryptographic module. This set of commands can be used only by the Crypto Officer or by Applet Providers having a Security Domain with Delegated Management privilege.

This set includes the following commands:

- ***INSTALL (CO):*** Install an application or a Security Domain. It requires invocation of different internal functions. The INSTALL command is used to instruct the Card Manager (or 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 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 Loaded File (package), an Application (applet instance) or a Security Domain.

Applets loaded onto the Cyberflex Access E-gate V3 cryptographic module must be FIPS 140-2 validated in order for the module to retain its FIPS validation.

Prior to applet loading, the Crypto Officer establishes a Secure Channel with the Card Manager during the identification/authentication process. The applet is divided into a series of blocks that fit in a LOAD command. 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 “GP 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 “GP 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 “GP DAP RSA” is a stronger mechanism. It verifies the integrity of the applet on behalf of the applet provider and it also authenticates applet provider as the originator of the applet.

5.2.2 Crypto Officer & User/Applet Provider services

Commands that are available for both the Crypto Officer and the User/Applet Provider are the following commands:

- **SELECT**: This command is used to select an application (Card Manager, Security Domain or Applet). Card Manager may be selected to load a Load File, to install an application loaded previously or to activate a Security Domain.
- **MANAGE CHANNEL**: This command is used for adding a new logical channel.
- **INITIALIZE UPDATE**: This command is used to initiate a Secure Channel with Card Manager or a Security Domain. The Cyberflex Access E-gate V3 cryptographic module and host session data are exchanged, and session keys are generated in the Cyberflex Access E-gate V3 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 Cyberflex Access E-gate V3 cryptographic module to authenticate the host, to establish a 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 DAP Public Key.
- **PUT RSA KEY**: This command is used to add a key set containing only the DAP or DM Public Key.
- **SET STATUS**: This command is used to modify the life cycle state of the Cyberflex Access E-gate V3 cryptographic module or the life cycle state of an application.
- **GET STATUS**: This command is used to retrieve Card Manager or Applications information according to a given search criteria.
- **STORE DATA**: This command is used to store or replace one tagged data object provided in the command data field.
- **GET DATA**: This command is used to retrieve a single data object. It is available outside the Secure Channel (no security condition). However, if issued within a Secure Channel, it must follow the same security level as defined in EXTERNAL AUTH. No CSPs are accessible with this command.
- **MASK TRACK**: This command allows reading of up to 10 traceability data bytes. It is used to determine that the module is in the FIPS Approved mode of operation.
- **GET SIZE**: This command is provided to retrieve the available EEPROM memory size.
- **CHANGE ATR**: This command allows modifying of the ATR.
- **READ SERIAL NUMBER**: This command is provided to retrieve 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 this access condition is checked on each received command.

The following services are unauthenticated: Select, Initialize Update, Manage Channel, Get Data, Read Serial Number, and Mask Track.

5.2.3 Relationship between Roles & Services

Roles / Services	Crypto-Officer (Card Manager Security Domain)	User/Applet Providers (Applet Security Domain)	Unauthenticated (Any role)	Algorithms
SELECT	X	X	X	
MANAGE CHANNEL	X	X	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
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
STORE 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

5.2.4 Services available for Applets

The Cyberflex Access E-gate V3 cryptographic module implements a secure environment for execution of User-developed applications, known as JavaCard Applets. Applets that are developed and downloaded onto the module shall use the Cyberflex Access E-gate V3 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 E-gate V3 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.
- 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 Number Generation:
  - Secure Random Generation: This API generates random data, using an ANSI X9.31 FIPS 140-2 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. Verification uses an RSA public key.
- Bulk Encryption/Decryption:
  - DES/TDES: These APIs offer DES/TDES CBC or ECB modes 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 an applet's validation. We recall that only FIPS 140-2 validated applets shall be loaded on the Cyberflex Access E-gate V3 cryptographic module.

5.2.4.1 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 Card Manager (Crypto Provider), a Security Domain, or in an Applet Security Domain.

5.2.5 Card Cryptographic Functions

The purpose of the Cyberflex Access E-gate V3 cryptographic module is to provide a FIPS Approved platform for applets that may in turn provide cryptographic services to end-user applications.

Keys represent the identity of the roles involved in controlling the Cyberflex Access E-gate V3 cryptographic module. DES, TDES, AES, RSA and SHA algorithms are provided as services to applets that may be loaded onto the Cyberflex Access E-gate V3 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 is subject to a separate validation involving applets. This Cyberflex Access E-gate V3 cryptographic module validation does not include such applets.

The Cyberflex Access E-gate V3 cryptographic module cryptographic functions are as follows:

- **DES [non-compliant]:**
  - DES is used together with TDES to compute a retail MAC, which is used as an EDC for the "GP DES DAP" and for the DM Receipt. Cf. 6.3.2. The DAP verification process does not provide any security relevant functionality as it relates to the FIPS 140-2 standard.

- DES functions are also provided as services to applets, through Java APIs. They shall be used only for legacy systems.

- **TDES, (2 keys TDES) [Cert# 468]:**
  - The TDES (TECB and TCBC modes) algorithm is used
    - to authenticate Crypto Officer (EXTERNAL AUTH command)
    - to encrypt 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 TDES MAC to authenticate the originator and to verify integrity of messages
  - 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 [Cert.#451]:**
  - AES (ECB and CBC modes) functions are only provided as services to applets through Java APIs.

- **SHA-1 [Cert# 514]:**
  - SHA-1 digest is used in the RSA signature.
  - It is used in the DAP and the DM.
  - SHA-1 digest is also provided as a service through Java APIs to applets.

- **SHA-256 [Cert# 514]:**
  - The SHA-256 function is only provided as a service through Java APIs to applets.

- **RSA (1024, 1536, 2048 bit keys) [vendor affirmed]:**
  - RSA is used for the "OP RSA DAP" as described in section 6.3.2.
  - RSA is used for the DM as described in section 6.3.3.
  - RSA is used as part of RSA SHA PKCS#1 signature.
  - RSA functions are also provided as services to applets, through Java APIs. The applet shall use RSA only for "key wrapping" (key establishment methodology provides between 80 and 112 bits of encryption strength) or "signature". This will be checked during the applet's FIPS validation.

- **RSA CRT SHA PKCS1 Signature (1024, 1536, 2048 bit keys) [Cert# 169]:**
  - RSA SHA PKCS1 Signature functions are provided as services to applets, through Java APIs.

- **RSA STD SHA PKCS1 Signature (1024, 1536, 2048 bit keys) [Cert# 170]:**
  - RSA SHA PKCS1 Signature functions are provided as services to applets, through Java APIs.

- **DRNG ANSI X9.31 [Cert# 236]:**
  - DRNG function is used to generate a nonce during the INITIALIZE UPDATE command.
  - It is provided as a service through Java APIs to applets.
  - It is also used in the RSA key generation provided as a service through Java APIs to applets.

- Hardware NDRNG
  - Used to generate the seed value and seed key for the ANSI X9.31 DRNG

5.2.6 Self-Tests

5.2.6.1 Power Up Self Tests

The Cyberflex Access E-gate V3 cryptographic module performs the required set of self-tests before executing any cryptographic operation. When a CAD interface powers the module up, the module sends (as specified by ISO/IEC 7816) an Answer To Reset (ATR) with static data about the module. It then waits for the first command.

When first command arrives, the module executes Self-Tests.

Self-Tests include:
- EEPROM Firmware integrity check with a CRC-16.
- Algorithm (known answer) tests for:
  - TDES- encrypt/decrypt (ECB and CBC)
  - AES- encrypt/decrypt (ECB and CBC)
  - SHA-1 Hashing,
  - SHA-256 Hashing,
  - RSACRT SHA PKCS1 sign and verify.
  - RSASTD SHA PKCS1 sign and verify.
  - DRNG
- Critical functions tests:
  - RAM functional test & clearing at power up
  - CRC-16 KAT performed at power up

If any of these tests fails, the Cyberflex Access E-gate V3 cryptographic module responds with a self-test error status. Then, the cryptographic module goes mute. No data of any type is transmitted from the cryptographic module to the CAD while self-tests are performed.

5.2.6.2 Conditional Tests

RSA Key generation:

A pair wise consistency check is performed during key generation. It is done in both directions: sign then verify for signature usage; encrypt then decrypt for key wrapping usage.

Note that this operation can only be activated by applets. It is therefore out of 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 FIPS 140-2 Approved deterministic RNG.

Software/Firmware load test

A TDES CBC MAC is verified whenever an applet is loaded onto the Cyberflex Access E-gate V3 cryptographic module. This MAC is linked to secure messaging.

An optional DAP verification is made. The algorithm used is an RSA signature or an algorithm using DES for the first n-1 blocks and a TDES for the last block.

5.3 CRITICAL SECURITY PARAMETERS (CSP):

5.3.1 Cryptographic Keys:

The Cyberflex Access E-gate V3 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 CO Card Manager Security Domain Key Set, used for OP authentication
3. TDES CO Card Manager Session Key Set
4. TDES Delegated Management (DM) Key

And in addition, the key sets of each applet Security Domain.
5. TDES User/Applet Provider (AP) Security Domain Key Set used for OP authentication
6. TDES User/AP Card Manager Session Key Set
7. TDES Data Authentication Pattern (DAP) Key

Keys #1, #2 & #4 are put in the Crypto-officer Security Domain key sets with the Put DES Key command.
Keys #3 & #6 are temporary keys stored in RAM.
Keys #5 & #7 are put in the User/AP Security Domain 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 key for Crypto Officer authentication and encrypted mode of the secure channel,
- K_{mac}, used to derive session key for Crypto Officer authentication and 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 E-gate V3 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.

5.3.2 Other CSPs

There are no other CSPs.

5.3.3 Public Keys

Public keys are not CSPs.

1. Delegated Management (DM) Public Key
2. Data Authentication Pattern (DAP) Public Key

Key #1 is put in the Crypto-officer Security Domain key sets with the Put RSA Key command.
Key #2 is put in the User/AP Security Domain 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 6.3.2 and 6.3.3.

6. SECURITY RULES

6.1 IDENTIFICATION & AUTHENTICATION SECURITY RULES

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

6.1.1 User Identification and Authentication

- **User/Applet Provider Authentication**: The User/Applet Provider must prove the possession of the TDES User/Applet Provider (AP) 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.

6.1.2 Cryptographic Officer Identification &Authentication

- **Crypto Officer Authentication**: Cryptographic Officer must prove the possession of the Cyberflex Access E-gate V3 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).

6.1.3 Attempt Counter

- **Attempt Counter**: An attempt counter is associated with each key set of a Security Domain or the Crypto-module Manager.
- **Initialization**: This counter is set to 3 at the creation of the key set and at each successful authentication using this key set.
- **Decrementation**: This counter is decremented by 1 at each unsuccessful authentication using this key set. When the counter reaches 0, the key set is blocked, which means that it cannot be used any more for authentication.

6.2 FIPS MODE OF OPERATION

The cryptographic module enforces FIPS mode of operation at all times.
This is asserted when the MASK TRACK command delivers an answer containing “03 01 01 01.”

6.3 APPLET LOADING SECURITY RULES

6.3.1 Integrity and Confidentiality of the loading

Only applets validated to FIPS 140-1 or 140-2 shall be loaded onto the Cyberflex Access E-gate V3 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 applet during its loading. 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.

6.3.2 Applet Loading with "GP 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 E-gate V3 cryptographic module provides a mechanism designated as "DAP" in [GP211] 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. DAP verification is done systematically at the end of loading, without any additional command.

The Cyberflex Access E-gate V3 cryptographic module provides two methods of DAP implementation, "GP DAP DES" and "GP DAP RSA". Only one of them is used when loading an applet.

- "GP DAP DES" works as an EDC that verifies 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 DES and TDES operations use 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.

- "GP DAP RSA" is a signature verification, which is a stronger mechanism than the "GP 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 the RSA PKCS#1 Signature of SHA-1 message Digest of the applet. 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.

6.3.3 Applet Loading with Delegated Management (DM)

In this case, the Applet provider loads his own applet. The Cyberflex Access E-gate V3 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 "GP DAP RSA" is an RSA signature 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.

6.4 ACCESS CONTROL SECURITY RULES

- Secret Keys are always loaded in encrypted form.

6.5 PHYSICAL SECURITY RULES

Physical security of Cyberflex Access E-gate V3 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 E-gate V3 cryptographic module is under control of the Cryptographic Officer until it is ultimately issued to the end user.

6.6 KEY MANAGEMENT SECURITY POLICY

6.6.1 Cryptographic key generation

- TDES Session keys for Secure Channel Opening, conforming to Open Platform Card Specification v2.1.1 using FIPS 140-2 Approved ANSI X9.31 DRNG.
- RSA key pair generation using FIPS 140-2 Approved ANSI X9.31 DRNG. Keys are generated in CRT format.

6.6.2 Cryptographic key entry/output

Secret Keys shall always be input in encrypted format, using the Put DES Key command. In this command, 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.

6.6.3 Cryptographic key storage

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).

6.6.4 Cryptographic key destruction

The Cyberflex Access E-gate V3 cryptographic module zeroizes 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.
Keys loaded for DAP and Delegated Management cannot be updated.
To zeroize DAP keys, their Security Domain must be deleted. This operation zeroizes all the keys contained in the Security Domain.
To delete DM keys, Cryptographic Module must be put in TERMINATED state. This operation zeroizes all keys in EEPROM. It is enabled by the Set Status command.

6.7 MITIGATION OF ATTACKS SECURITY POLICY

The Cyberflex Access E-gate V3 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 (2-key)	TDES keys (Crypto Officer Security Domain)
User/Applet Provider	TDES authentication (2-key)	TDES keys (User/AP 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 5.2.1 CO & User Services as listed in Section 5.2.2
User/Applet Provider	CO & User Services as listed in Section 5.2.2. APIs as listed in Section 5.2.4.

7.4 ACCESS RIGHTS WITHIN SERVICES

CSP	Service	Role	Types of Access
TDES CO Card Manager Security Domain Keys	PUT DES KEY command	Crypto Officer	Write
TDES CO Card Manager Security Domain Keys	INITIALIZE UPDATE & EXTERNAL AUTH	Crypto Officer	Execute
TDES CO Card Manager Security Domain Key: K_{KEK}	PUT KEY command (encryption of the key)	Crypto Officer	Execute
TDES CO Card Manager Session Keys	INITIALIZE UPDATE & EXTERNAL AUTH	Crypto Officer	Create
TDES CO Card Manager Session Key: K_{enc}	Message encryption	Crypto Officer	Execute
TDES CO Card Manager Session Key: K_{mac}	Message integrity	Crypto Officer	Execute
TDES DM Key	PUT DES KEY command	Crypto Officer	Write
TDES DM Key	DM Receipt computation	Crypto Officer	Execute
TDES User/AP Security Domain Keys	PUT KEY command	User	Write
TDES User/AP Security Domain Keys	INITIALIZE UPDATE & EXTERNAL AUTH	User	Execute
TDES User/AP Security Domain Key: K_{KEK}	PUT KEY command (encryption of the key)	User	Execute
TDES User/AP Card Manager Session Keys	INITIALIZE UPDATE & EXTERNAL AUTH	User	Create
TDES User/AP Card Manager Session Key: K_{enc}	Message encryption	User	Execute
TDES User/AP Card Manager Session Key: K_{mac}	Message integrity	User	Execute
TDES DAP Key	PUT DES KEY command	User	Write
TDES DAP Key	“GP DAP” verification	User	Execute

Public Keys	Service	Role	Types of Access
DM Public Key	PUT RSA KEY command	Crypto Officer	Write
DM Public Key	DM DAP verification	Crypto Officer	Execute
DAP Public Key	PUT RSA KEY command	User	Write
DAP Public Key	“GP 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
[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
[JCVM221]	Java Card ™ 2.2.1 Virtual Machine Specification, Sun Microsystems
[JCAPI221]	Java Card ™ 2.2.1 Application Programming Interface, Sun Microsystems
[JCRE221]	Java Card ™ 2.2.1 Runtime Environment (JCRE) Specification, Sun Microsystems
[GP211]	Global Platform Card Specification v 2.1.1 - march 2003
[ISO 7816-1]	ISO/IEC JTC 1/SC 17/WG4 Integrated circuits() cards with contacts – Part 1: Physical Characteristics
[ISO 7816-2]	ISO/IEC JTC 1/SC 17/WG4 Integrated circuits() cards with contacts – Part 2: Dimension and Location of the contacts
[ISO 7816-3]	ISO/IEC JTC 1/SC 17/WG4 Integrated circuits() cards with contacts – Part 3: Electronic signals and transmission protocol
[ISO 7816-4]	Identification cards - Integrated circuit(s) cards with contacts - Part 4: Inter-industry commands for interchange
[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.
[FIPS 197]	FIPS-197: Advanced Encryption Standard (AES)
[FIPS 46-3]	FIPS-46-3: Data Encryption Standard (DES)
[SP 800-38 A]	NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of operation
[FIPS 180-2]	FIPS-46-3: Secure Hash Standard (SHA)
[RSA PKCS#1]	PKCS #1 v2.1: RSA Cryptography Standard
[ISO 9796-2]	ISO/IEC 9796-2
[USB]	Universal Serial Bus Specification v 1.1

9. ACRONYMS

Acronyms	Definitions
AES	Advanced Encryption Standard
ANSI	American 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
CSP	Critical Security Parameter
DAP	Data Authentication Pattern
DEA	Data Encryption Algorithm (formerly DES)
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
GP	Global Platform
PC	Personal Computer
PCD	Proximity Coupling Device
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standards
RAM	Random Access Memory
RFU	Reserved for Future Use
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest Shamir Adelman
SHA	Secure Hash Algorithm
SPA	Simple Power Analysis
TDES	Triple-DES