KEYCORP LIMITED

Keycorp MULTOS I4F 80K with MULTOS PIV Card Application FIPS 140-2 Level 2

Security Policy

Author: Keycorp Ltd.

Document Number: SIM-SP-0304 **Date: September 2008**
Revision Number: 1.3.1

Table of Contents

1. Introduction **3**

2. Module Overview **4**

2.1 Keycorp MULTOS I4F 80K Chip Platform *4*
2.1.1 Operational Environment 6
2.1.2 MULTOS PIV Card Application 6

2.2 Security Level *6*

3. Cryptographic Module Specification **7**

3.1 Cryptographic Module Ports and Interfaces *7*

3.2 Module Interfaces *8*
3.2.1 ISO7816 Contact Interface 8
3.2.2 ISO14443 Contactless Interface 8

3.3 Logical Interfaces *9*

4. Roles, Authentication & Services **10**

4.1 Roles *10*
4.1.1 Cryptographic Officer Roles 10
4.1.2 User Roles 10

4.2 Role Authentication and Authentication Strength *10*
4.2.1 PIV Card Holder 10
4.2.2 PIV Card Application Administrator 10
4.2.3 PIV Card User PIN Administrator 11

4.3 Services *11*

5. Cryptographic Functions **12**

6. Critical Security Parameters **13**

7. Security Rules **14**

7.1 FIPS Mode of Operation *14*

7.2 Physical Security Rules *14*

7.3 Key Management *14*

8. Self Tests **16**

Abbreviations and acronyms **18**

1. Introduction

This document defines the non-proprietary Security Policy for the KEYCORP MULTOS I4F 80K with MULTOS PIV Card Application, which is a dual interface single chip cryptographic module, submitted for testing for FIPS 140-2 Level 2 requirements.
In this document the term *Cryptographic Module* refers to the KEYCORP MULTOS I4F 80K with MULTOS PIV Card Application. The term *MULTOS* refers to the Keycorp MULTOS smartcard operating system within the Cryptographic Module. The term MULTOS *PIV Card Application* refers to the two component applications that make up the MULTOS PIV Card Application within the Cryptographic Module.
Included in this document is a description of the security requirements for the Cryptographic Module and a qualitative description of how each security requirement is achieved. This Security Policy also specifies the security rules under which the Cryptographic Module must operate.

2. Module Overview

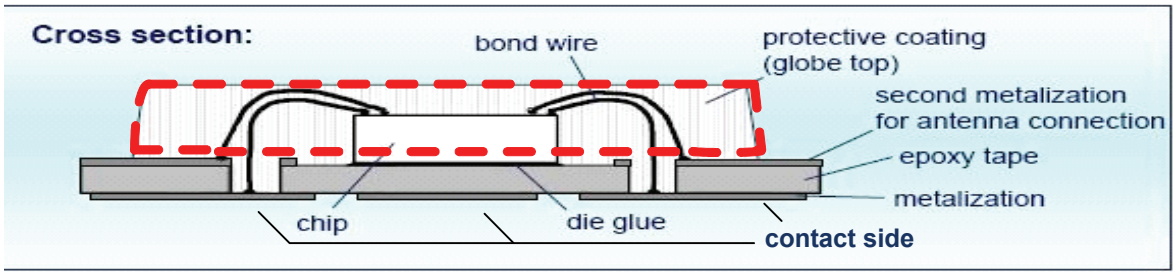
2.1 Keycorp MULTOS I4F 80K Chip Platform

KEYCORP MULTOS I4F 80K with MULTOS PIV Card Application:
Hardware version: SLE66CLX800PEM
Firmware version: 1.0
PIV Certificate # 5
The KEYCORP MULTOS I4F 80K with MULTOS PIV Card Application is made up of the KEYCORP MULTOS I4F 80K chip platform with the MULTOS PIV Card Application.
The following section provides an overview of both components.

The Cryptographic Module is a single-chip, limited operational environment, smartcard module containing a microprocessor, EEPROM, and RAM with dual interface (contact and contactless).
The Cryptographic Module consists of a smartcard module based on an Infineon SLE66CLX800PEM microcontroller, the Keycorp MULTOS smartcard operating system contained in ROM memory, with MULTOS configuration information in EE memory together with an application in EE memory, the MULTOS PIV Card Application. MULTOS provides a limited operational environment for the Cryptographic Module. The MULTOS configuration can be determined by the GET MANUFACTURER DATA and GET MULTOS DATA commands.
MULTOS is an operating system for integrated circuit cards (also known as smartcards). The user of the smartcard accesses the applications on it via an Interface Device (IFD), which could be a Point-of-Sale terminal, Automatic Teller Machine, or some other device which supports ISO 7816 contact smartcard protocols or ISO14443 contactless protocols.
Communications across the IFD-MULTOS interface comprise a message transmitted by the smartcard when it is reset, followed by command-response pairs, where a command is a message from the IFD to MULTOS and a response is a message from MULTOS to the IFD.
By means of these command-response pairs, MULTOS allows:
An IFD to access data and applications which are on the card.
a) Information specific to the card to be retrieved by an IFD.
MULTOS is a single-threaded operating system. Only one application can be executing at any given time. MULTOS does not provide mechanisms for concurrency or multi-tasking. Following power-on of the smartcard and initialisation, the basic execution sequence for MULTOS is as follows:
a) Wait for input from the IFD.
Parse the input.
If the input is a MULTOS command, process the command and write a response to the IFD.
Otherwise, execute the currently selected application and write to the IFD any output created by the application.
Loop back to a).
Applications to be loaded on MULTOS-based smartcards are written in a hardware-independent language called MULTOS Executable Language (MEL). MEL applications are interpreted by MULTOS, rather than being compiled and executed directly on the smartcard processor.
MULTOS also provides for shared code routines, called Codelets, which can be called by an executing application. Codelets can be loaded into MULTOS during IC manufacture or at smartcard personalisation time. A codelet has its own code address space but executes in the context of the calling application, so has access to the application's data.
The Cryptographic Module is implemented on a single-chip smartcard microcontroller which consists of the following elements:
– Five pins which allow the interface device (IFD) to communicate with the Cryptographic Module as follows:

VCC and GND, which supply power to the Cryptographic Module.
RESET, which is used by the IFD to reset the Cryptographic Module.
I/O, a bi-directional serial channel along which commands and responses are sent using standardised communication protocols.
CLK, which is used to supply the SLE66CLX800PEM processor with a clock.
– Two pins which allow the attachment of a loop antenna which allow the coupling of power into the Cryptographic Module and input commands into the Cryptographic Module and which also allow the Cryptographic Module to modulate the coupled signal to allow communication from the Cryptographic Module to the IFD.
– mask ROM.
– EEPROM (including a 32-byte Security PROM and one-time programmable (OTP) area).
– RAM.
– A 1100-bit crypto co-processor used to support public key cryptographic algorithms.
– A hardware random number generator (used to seed the software FIPS Approved Pseudo RNG).
– A timer with prescaler.
– A CRC module.
– A memory management protection unit.
– A phased locked loop unit.
– An interrupt module (interrupts unused).
– A UART.
– A 112-Bit / 192-Bit DDES-EC2 Accelerator.

The red dotted line in the diagram below illustrates the module cryptographic boundary.
The Cryptographic Module boundary is the physical boundary of the single-chip microprocessor.
The epoxy glue and the support on which the crypto module is glued (contact plate or antenna) are not part of the crypto module boundary.



2.1.1 Operational Environment

The Cryptographic Module has a Limited Operational Environment.

2.1.2 MULTOS PIV Card Application

The MULTOS PIV Card Application has been developed to provide a Personal Identity Verification Card (PIV) validated to FIPS 140-2 and FIPS 201. The MULTOS PIV Card Application implements the requirements for the retrieval and usage of the identity credentials from a PIV card.
FIPS 201 employs cryptographic mechanisms to authenticate cardholders, to secure information stored on the PIV Card, and to secure the supporting infrastructure.
FIPS 201 and its supporting documents specify a suite of keys to be stored on the PIV Card for personal identity verification, digital signature generation, and key management. The Cryptographic Module supports various roles with the rights to use the cryptographic keys to perform card or cardholder authentication and access to card objects.
The PIV application also includes a command to retrieve the version information for the application itself. This makes it possible to determine that the PIV application being used matches this security policy.

2.2 Security Level

The Cryptographic Module meets the overall requirements applicable to Level 2 security of FIPS 140-2. The Cryptographic Module supports a Limited Operational Environment as defined in FIPS 140-2.

Security Requirements Section	Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self Tests	2
Design Assurance	2
Mitigation of other attacks	N/A

3. Cryptographic Module Specification

The Cryptographic Module supports authentication of the PIV Card Application to a PIV Card Application Issuer, authentication of a PIV Card Holder to the PIV Application, digital signing of documents by the PIV Card Holder, and management of cryptographic keys and digital certificates within the PIV Application by a PIV Application Administrator.
Access to cryptographic services provided by the Cryptographic Module is controlled by a role based access control policy following the result of authentication of an entity.
The PIV Application offers services to middleware external to the Cryptographic Module, relying on secure memory management and cryptographic services provided by the Cryptographic Module.
The services are activated with “APDU commands” sent to the Cryptographic Module.
The PIV Application is responsible for key management of all keys associated with the PIV functionality.
The following functional block diagram shows the main components of the Cryptographic Module.

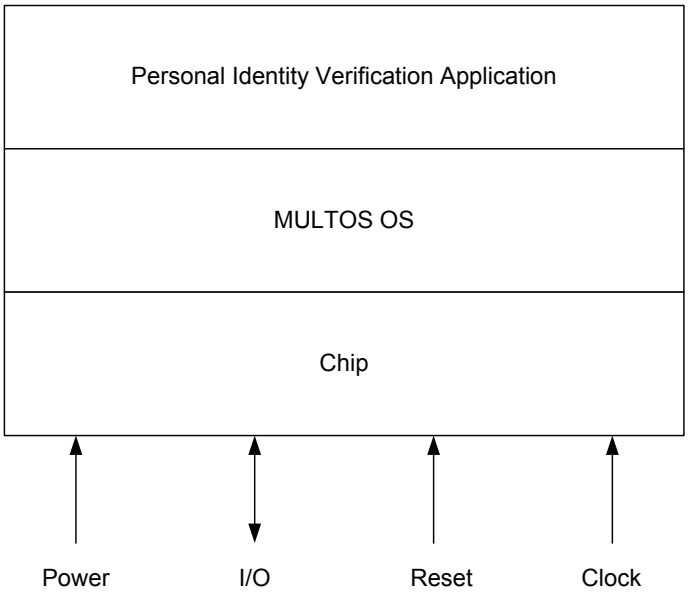


Figure – Functional Block Diagram

The Cryptographic module operation is partitioned into two modes, one when operating via the contactless interface and the other when operating via the contact interface. All cryptographic mechanisms are accessible via the contact interface but certain cryptographic mechanisms are not accessible via the contactless interface (see later section, Cryptographic Functions).

3.1 Cryptographic Module Ports and Interfaces

The integrated circuit used in the KEYCORP MULTOS I4F 80K with MULTOS PIV Card Application is a single chip that supports both a contact interface and a contactless interface.

3.2 Module Interfaces

The Cryptographic Module supports the following interfaces:
ISO/IEC 7816: Identification Cards – Integrated Circuit Cards with Contacts.
ISO/IEC 14443: Identification Cards – Contactless Integrated Circuit Cards – Proximity cards.
The Cryptographic Module supports seven electrical connections. Five are via wire bonds to the externally visible contact plate and conform to the ISO7816-2 standard. These five connections are:

Contact	Purpose
VCC	Power supply positive connection
GND	Power supply ground connection
RST	Reset
CLK	Clock
I/O	Data Input / Output

The I/O connection is used for bi-directional communications and this single pin supports the Command Input, Status Output and Data Input and Data Output functions of the Cryptographic Module. These various functions are dependent on the ISO7816 command being processed by the Cryptographic Module, see later.
The further two connections to the module are to the face opposite to the external contact face and these two connections mate to a loop antenna to allow contactless communications with the module. When operating in a contactless mode the antenna both provides power to the module and allows bi-directional communication with the module. Refer to ISO14443 for details.

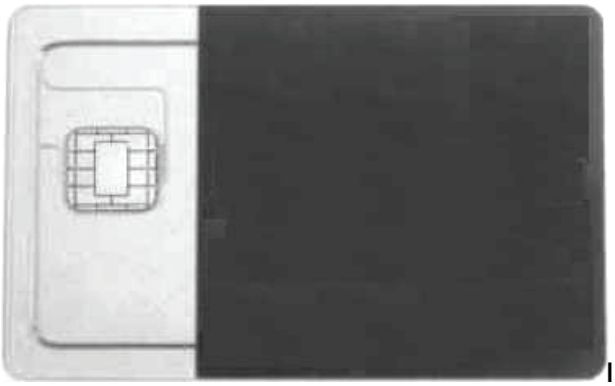
3.2.1 ISO7816 Contact Interface

Protocols: ISO7816 T=0, T=1; PPS.
Communications speeds up to 447kbit/s.
Supply voltage range: 5V ± 10% (Class A), 3V ± 10% (Class B)
Current consumption < 10 mA @ 5.5 V
External CPU clock frequency: 1 to 7.5 MHz
Internal CPU clock frequency: up to 30MHz
ESD protection 6KV maximum
The module figure in the earlier Module Overview section shows the contacts of the Cryptographic Module. The external contact plate conforms to the ISO7816-2 standard.

3.2.2 ISO14443 Contactless Interface

Protocols: ISO14443 Type A or Type B.
Communications speeds up to 848kbit/s with both Type A and B.
Carrier frequency 13.56 MHz

The following figure shows the relationship between the Cryptographic Module and the loop antenna within the card housing. The loop antenna is connected to the second metallisation as in the figures of the prior section. In the example figure the blue overlay that sandwiches the loop antenna has been cut-away over a portion of the loop antenna. The card plastic and loop antenna are external to the Cryptographic Module physical boundary.



3.3 Logical Interfaces

Once contact is established between the cryptographic module and the card reader, the cryptographic module functions as a “slave” processor to implement and respond to the card reader commands. The cryptographic module adheres to a well-defined set of state transitions. Within each state, a specific set of commands is accessible.
Both contact and contactless interfaces are routed to a common logical command/response interface with command and response data conforming to the ISO7816-4 standard.

Logical Interface	Physical Interface
Data In	**Pin C7 of the module and Antenna interface on the underside of the module**
Data Out	**Pin C7 of the module and Antenna interface on the underside of the module**
Control In	**Pins C2, C3, C7 of the module and Antenna interface on the underside of the module.**
Status Out	**Pin C7 of the module and Antenna interface on the underside of the module**

4. Roles, Authentication & Services

4.1 Roles

The KEYCORP MULTOS I4F 80K with MULTOS PIV Card Application supports Crypto Officer and User Roles. The cryptographic module does not implement a maintenance role.

4.1.1 Cryptographic Officer Roles

PIV Card Application Administrator – the administrator of key material on the card.
The PIV Card Application Administrator role is able to generate new RSA keys and update card data objects including X509 certificates.
PIV Card User PIN Administrator – the administrator of the Card Holder PIN on the card.
The PIV Card User PIN Administrator role is able to reset the Card Holder PIN.

4.1.2 User Roles

PIV Card Holder – the owner of the cryptographic module. The PIV Card Holder role is responsible for not communicating their PIN to other parties.

4.2 Role Authentication and Authentication Strength

4.2.1 PIV Card Holder

Knowledge of a PIN is the means by which the PIV Card Holder is authenticated to the PIV Card Application. The PIN interface requires an 8-character PIN.
The probability of guessing the PIN in a single try is one in 10^8 (one-hundred million).
A retry counter is associated with the PIN of the PIV Application. The PIN retry counter is set to 3 at the creation of the PIV Application and when a correct PIN is presented for Card Holder verification. The PIN retry counter is also reset to 3 when the PIV Card Application Administrator has been authenticated and a correct PUK value is supplied as part of a RESET RETRY COUNTER command. The retry counter is decremented when an incorrect PIN is presented.
When the counter reaches 0 the associated PIN is disabled, thereby disabling Card Holder authentication and any associated mechanisms.
The retry counter is stored in non-volatile memory to guarantee that invalid PIN entries accumulate correctly and will not get lost between card sessions.

4.2.2 PIV Card Application Administrator

Knowledge of a Triple-DES secret key is the means by which the PIV Card Application Provider is authenticated to the PIV card application. A random challenge from the card application will be encrypted with 168bit key Triple-DES-ECB by the PIV Card Application Provider and the result passed to the Cryptographic Module. Decryption and check of the result by the Cryptographic Module will authenticate the PIV Card Application Provider.
The probability of guessing the key in a single try is one in 2^168.
The authentication request must occur immediately after requesting the challenge. Any other command will invalidate the authentication request. The security state is kept in volatile session memory to ensure that any card reset or re-select of the PIV application will invalidate the authentication level.

4.2.3 PIV Card User PIN Administrator

Knowledge of a PUK is the means by which the PIV Card User PIN Administrator is authenticated to the PIV Card Application. The PUK is presented as a component of the RESET RETRY COUNTER command. The PIV Card User PIN Administrator is only authenticated for the duration of this command.
The RESET RETRY COUNTER command requires an 8-character PUK which exceeds the requirement of providing better than a 1 in 1,000,000 chance of a successful random attempt.
A retry counter is associated with the PUK of the PIV Application. The PUK retry counter is set to 10 at the creation of the PIV Application and when a correct PUK is presented in a RESET RETRY COUNTER command. The retry counter is decremented when an incorrect PUK is presented.
When the counter reaches 0 the associated PUK is disabled, thereby disabling the RESET RETRY COUNTER mechanism. The retry counter of 10 together with less than 1 in 1,000,000 chance of guessing a PIN ensures that there is a less than a 1 in 100,000 chance that a random PIN will be successful in a one minute period.

4.3 Services

The Cryptographic Module provides the following services:

Role	Service	CSP	Access
PIV Card Application Administrator (C-O)	**CHANGE REFERENCE DATA**	**TDES key 9B**	**Write once**
	GENERATE ASYMMETRIC KEYPAIR	**RSA 1024/2048 bit key**	**Write**
	GET DATA	**N/A**	**N/A**
	PUT DATA	**N/A**	**N/A**
	SELECT	**N/A**	**N/A**
PIV Card User PIN Administrator (C-O)	**CHANGE REFERENCE DATA**	**PUK**	**Write**
	GET DATA	**N/A**	**N/A**
	RESET RETRY COUNTER	**PIN**	**Write**
	SELECT	**N/A**	**N/A**
	VERIFY	**PUK**	**On card process**
PIV Card Holder (User)	**CHANGE REFERENCE DATA**	**PIN**	**Write**
	GENERAL AUTHENTICATE (Non-FIPS Approved)	**RSA 2048 bit key, TDES key**	**On card process**
	GET DATA	**N/A**	**N/A**
	SELECT	**N/A**	**N/A**
	VERIFY	**PIN**	**On card process**
Unauthenticated	**SELECT**	**N/A**	**N/A**
	PUT DATA	**N/A**	**N/A**
	GET DATA	**N/A**	**N/A**

5. Cryptographic Functions

The Cryptographic Module provides cryptographic services to end-user applications. Cryptographic keys and PINs form the basis of role authentication and these keys and other keys form the basis of cryptographic functions at the Cryptographic Module interface.

The cryptographic algorithms and purpose are:

Triple-DES-ECB (Cert.# 605): This algorithm uses the uses the PIV Card Application Administration Key (see CSP section) and the GENERAL AUTHENTICATE command for authentication of the PIV Card Application Administrator role. The GENERAL AUTHENTICATE with this key can also be used to authenticate the card over the contact or contactless interface. Triple-DES-ECB is a FIPS-approved algorithm, refer FIPS 46-3.

RSA PKCS1 2048bit (Cert.# 303): Used to sign data using the GENERAL AUTHENTICATE command.
This is a FIPS-approved algorithm, refer FIPS 186-2.

Random Number Generator (RNG) (Cert.# 376): This algorithm is a Deterministic Random Number Generator (DRNG) seeded by a hardware random number generator. The DRNG complies with ANSI X9.31 which is a FIPS-approved algorithm, refer FIPS 186-2.

The Cryptographic Module provides the following non-Approved cryptographic algorithms.

Hardware RNG: Used to seed Random Number Generator (ANSI X9.31)

DES: Not for use in FIPS mode

RSA AHASH: Not for use in FIPS mode.

NOTE: The SHS is not implemented by the PIV application. The PIV application assumes host-side hash as specified in FIPS 201-1 (4.3).

6. Critical Security Parameters

Algorithm Type	SP800-73 Key Ref	Key Reference Name	Authenticated Entity	Contact/Contactless
PIN	80	Card Holder PIN	Card Holder	Contact
PUK	N/A	PIV Card PIN Unblocking Key (PUK)	PIV Card Application Administrator	Contact
RSA PKCS1 1024/2048	9A	PIV Authentication Key	(1) PIV card Application Provider	Contact
Triple-DES	9B	PIV Card Application Administration Key	(2) PIV Card Application Administrator	Contact/Contactless

The Cryptographic Module allows cryptographic protocols using asymmetric keys that require PIN on the contact interface and not the contactless interface. Therefore, of the PIV keys, only the Triple-DES PIV Card Application Authentication Key (SP800-73 key reference 9B) can be accessed via the contactless interface.
(1) [mandatory] Key 9A can be used to sign input data as a component of a GENERAL AUTHENTICATE command but authentication using this key does not gate access to any functionality within the Cryptographic Module. Key 9A is only accessible once the PIV Card Holder has been authenticated by their PIN and is only available over the contact interface.
(2) [mandatory] Key 9B is available for GENERAL AUTHENTICATE at any time while the PIV application of the Cryptographic Module is active and is available over both contact and contactless interfaces.
(3) [optional] Keys 9C, 9D and 9E have not been tested and are not part of this FIPS implementation.

7. Security Rules

7.1 FIPS Mode of Operation

The following is required for the module to be used in FIPS-mode.

The eight (8) character PIN length is hard-coded and enforced whenever a PIN is being used.
No additional configuration is necessary.

The eight (8) character PUK length is hard-coded and enforced whenever a PUK is being used.
No additional configuration is necessary.

Only FIPS Approved algorithms may be used.

7.2 Physical Security Rules

The Cryptographic Module embodiment is single-chip. The FIPS 140-2 Level 3 physical security requirements are met through the use of a hard potting material which surrounds the circuitry of the smart card chip. Attempts to pry off the contact plate or otherwise breach the chip's potting material to gain access to the internal chip circuitry will result in permanent damage to the Cryptographic Module, rendering it inoperative. The physical security requirements of the module are also met using the Active Shield feature with automatic and user controlled attack detection.
The PIV card plastic housing with embedded antenna for contactless operations is outside the Cryptographic Module boundary and beyond the scope of this Security Policy.

The contactless antenna interface connects to the Cryptographic Module through physical interface ports on the smart card chip. Any direct access to the contactless antenna or connection points to the Cryptographic Module reveals no additional information that could not be gained by reception of the contactless transmissions.

7.3 Key Management

7.3.1.1 Key Generation

RSA PKCS#1 key pair generation using FIPS 140-2 approved ANSI X9.31 DRNG for prime number generation. The keys are generated in RSA CRT format and stored in the PIV application data space. The PIV Card Issuance and Management subsystem loads the Triple-DES key on the card.

7.3.1.2 Cryptographic key entry/output

Key material is neither imported nor exported to/from the Cryptographic Module.

7.3.1.3 Cryptographic key storage

All PIN and key material listed in the table of Critical Security Parameters are stored in EEPROM memory in the PIV application data space in cleartext format. There are no unauthenticated interfaces to any CSPs stored within the module boundary.

7.3.1.4 Cryptographic key destruction

(1) The Cryptographic Module destroys RSA cryptographic keys by overwriting with another keyset using the GENERATE ASYMMETRIC KEY PAIR command. The PIV Card Application Administrator is the only role that can issue this command. No other mechanisms are provided for RSA key re-initialization or Triple-DES key re-initialization.

(2) Any key, including the Triple-DES key can be physically destroyed when calling the GENERATE ASYMMETRIC KEY PAIR service with “zeroize keys” parameter. This option kills all keys by overwriting them with zeroes. During the same session, new, asymmetric keys can be generated.

(3) The PIV Authentication key (RSA) and PIV Card Application Administration Key (TDES) can be zeroized by deleting the PIV application. On receipt of a valid application delete request MULTOS erases EE memory associated with the application. Zeroization requires authentication with the 9B key. Triple-DES keys are erased in approximately 3 milliseconds.

8. Self Tests

If the Cryptographic Module is reset or loses power while processing a command or executing an application, the Cryptographic Module will perform the Power On Self Tests (POSTs) prior to any Data Output from the Cryptographic Module:

Firmware Integrity Test: EDC.

Known Answer Tests: Triple-DES, DRNG (ANSI X9.31).

Known Answer Test: RSA PKCS#1 Signature.

The module also performs the following Continuous Self Tests:

Continuous RNG Tests: DRNG (ANSI X9.31) and Hardware Random Number Generator.

Pairwise Consistency Check: RSA.

If any test fails, the Cryptographic Module will become mute (inhibit all output) until reset.

References

ISO/IEC 7816: Identification Cards – Integrated circuit cards with contacts.
[ISO 7816-2]: Integrated circuit cards with contacts – Dimensions and locations of the contacts.
[ISO 7816-3]: Integrated circuit cards with contacts – Electrical interface and transmission protocols.
[ISO 7816-4]: [ISO 7816-3]: Integrated circuit cards with contacts – Organization, security and commands for interchange.
[ISO 14443]: Identification cards ― Contactless integrated circuit(s) cards ― Proximity cards.
[ANSI X9.31]: American National Standards Institute, American Bakers Association, Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), ANSI X9.31, 1998.
[SP-800-73-1]: Interfaces for Personal Identity Verification, April 2006.
[FIPS PUB 201-1]: Federal Information Processing Standard, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006.
[FIPS PUB 46-3]: Federal Information Processing Standard, Data Encryption Standard (DES), October 1999.
[FIPS PUB 186-2]: Federal Information Processing Standard, Digital Signature Standard (DSS), January 2000.
[FIPS 140-2]: National Institute of Standards and Technology, Federal Information Processing Standard 140-2, Security Requirements for Cryptographic Modules.

Glossary

Abbreviations and acronyms

Term	Description
ABEND	**Abnormal End (MEL application or MULTOS execution) card is then mute.**
ADC	**Application Delete Certificate.**
APDU	**Application Protocol Data Unit.**
ALC	**Application Load Certificate.**
ALU	**Application Load Unit.**
ATR	**Answer To Reset.**
CSP	**Critical Security Parameter.**
EEPROM	**Electrically Erasable Programmable Read Only Memory.**
IC	**Integrated Circuit.**
IFD	**Interface Device (to smartcard).**
MEL	**MULTOS Executable Language (application language).**
MSM	**MULTOS Security Manager.**
PIN	**Personal Identification Number.**
PIV	**Personal Identity Verification.**
PUK	**PIN Unblocking Key.**
RAM	**Random Access Memory.**
ROM	**Read Only Memory.**
RSA	**Rivest-Shamir-Aldeman (algorithm).**
Triple-DES	**3 key Triple DES.**