Personal Identity Verification Application on HITACHI MULTOS Smart Chip

Hardware Version: AE45X1
Firmware Version: 1.0

FIPS140-2 (Level 2)

Cryptographic Module Security Policy

Version 4.0

October 12th, 2006

Table of Contents

1. INTRODUCTION

This document defines the Security Policy for “Personal Identity Verification Application on HITACHI MULTOS Smart Chip cryptographic module, submitted for validation, in accordance with FIPS140-2 Level 2 requirements.

Included are a description of the security requirements for the 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. This document describes the security policy when the module is configured for FIPS 140-2 Level 2 operation.

2. OVERVIEW

2.1 Hitachi MULTOS Smart Chip

The HITACHI MULTOS Smart Chip is a single chip module that is designed to be embedded within a plastic card embodiment to provide an ISO-7816 compliant smart card with dual interface (contact and contactless), which is compliant with MULTOS.

The MULTOS is high-security multi-application smart card operating system and Key Management Infrastructure provides Card Issuers with the opportunity to define their own card programmes, delivering services with their own smart card applications or those of other third-party Application Providers. The MULTOS OS is part of firmware build 1.0.

MULTOS includes the “Application Abstract Machine”, a virtual machine environment. The virtual machine gives each application its own safe and secure operating environment, separated from those of other applications by the so-called “firewall”. MULTOS Applications contain actions, developed in a language known as MEL (MULTOS Executable Language) that is processed one-by-one by the Virtual Machine. However, before being processed, each MEL action is verified by the Virtual Machine to ensure that it does not attempt an illegal operation, for instance, to attempt to read another application’s data or to attempt to amend its own programming. On MULTOS, the verification is performed during the application run-time, which means that even if an illegal programming action is attempted, the virtual machine will stop the illegal action from being executed. The run-time verification of each and every action of an application gives different Application Providers complete confidence that MULTOS is continually checking that their and other applications do not illegally interact.

In addition, whether embedded into a plastic card, the Hitachi MULTOS Smart Chip cryptographic module hardware provides tamper resistance and tamper evidence features that meet FIPS 140-2 LEVEL 3 physical requirements.

The Figure 1 shows an example the integrated Circuit (micro-controller) and the golden wires underneath the epoxy resin.

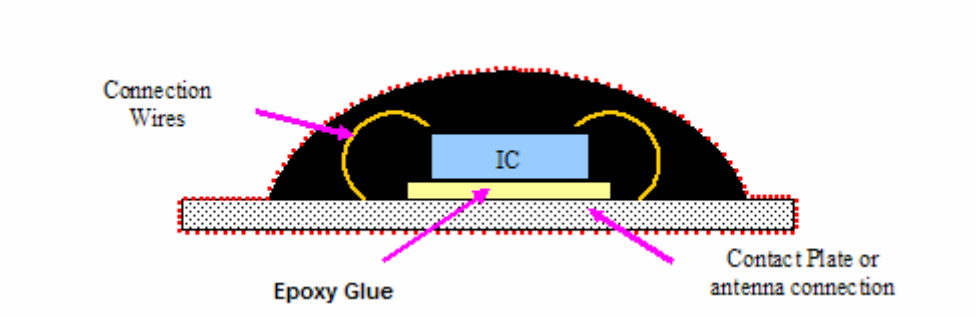

Figure 1: Example of the micro-controller and the golden wires underneath the epoxy resin

The red dotted line shows the module cryptographic boundary.

This cryptographic module consists of the following elements:

(1) Renesas Technology Corp. AE45X1, hardware version is HD65145X1,16bit microcontroller. This IC chip is a standard, production-quality.

(2) This IC chip includes ROM, RAM, and EEPROM.

(3) Operating system software and Personal Identity Verification Application are installed on ROM and EEPROM of this IC chip to provide processing capabilities and data storage and behavior as MULTOS card.

This document is submitted for validation of the module in accordance with FIPS 140-2 Level 2 standard.

2.2 PERSONAL IDENTITY VERIFICATION APPLICATION

The Personal Identity Verification Application:

• Provides enhanced functionality, flexibility and security based on the MULTOS.

• Conforms to FIPS 201 specification.

3. SECURITY LEVEL

The Personal Identity Verification Application on Hitachi MULTOS Smart Chip is designed and implemented to meet the Level 2 requirements of FIPS140-2. This document describes the module FIPS 140-2 Level 2 security policy.

The individual security requirements specified for FIPS 140-2 meet the level 2 specifications indicated in the Table 1.

Table1 –Security Requirements Specific to FIPS 140-2

Security Requirements Section	Level
Cryptographic module specification	2
Cryptographic module ports and interfaces	2
Roles, services, and authentication	3
Finite state model	2
Physical security	3
Operational environment	N/A
Cryptographic key management	2
EMI/EMC	3
Self tests	2
Design assurance	3
Mitigation of other attacks	N/A

4. CRYPTOGRAPHIC MODULE SPECIFICATION

The Personal Identity Verification Application on Hitachi MULTOS Smart Chip supports identity-based authentication of the Card Holder, using a PIN and identity-based authentication of the Card Application Administrator by possession of a triple DES key.

This validation effort is aimed at the systems software, virtual machines, and Personal Identity Verification Application.

The Personal Identity Verification Application byte code is loaded in the cryptographic module memory to use the MULTOS scheme. This function is performed at the manufacturing.

The application offers services to external applications, relying on key management, secure memory management and cryptographic services, provided by the cryptographic module. The services are performed with “APDU commands” sent to the cryptographic module.

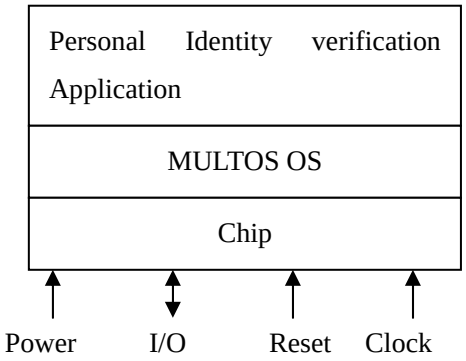

Figure 2: Functional block diagram

4.1 MODULE INTERFACES

This 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 Personal Identity Verification Application on Hitachi MULTOS Smart Chip was tested using both interfaces.

4.1.1 ISO/IEC 7816 Physical Interface (contact mode)

4.1.1.1 Interface Physical Specifications

In this contact mode, communication to and from the cryptographic module is done through a card contact (contact plate) that provides the electrical connection required. Five electric wires connect the module to the card contact. The card contact itself is outside of the module cryptographic.

Hitachi MULTOS Smart Chip operates in both ISO 7816-3 class A and class B. Class A requires a power supply voltage between 4.5 Volt and 5.5 Volt. Class B requires a power supply voltage between 2.7 Volt and 3.3 Volt.

4.1.1.2 Interface Electrical Specifications

The card contacts were the five electrical connections from the module are wire bonded to the contact plate.

The five electrical signals transmitted to the module through the contact mode wires coming from the contact plate are shown in Table 2.

These connected five electronic signals are in full compliance with the ISO/IEC 7816-3 standard.

Table 2 –Functional Specifications of Chip Contacts

Contact	Function	FIPS 140 Logical Interface
C1	Vcc supply voltage 2.7 to 5.5	Power Interface
C2	RST (Reset)	Control Input Interface
C3	CLK (Clock)	Control Input Interface
C4	Not Connected to the chip	N/A
C5	GND (Ground)	Power Interface
C6	Not Connected to the chip	N/A
C7	I/O bi-directional data line	Data Input Interface, Data Output Interface, Control Input Interface Status Output Interface
C8	Not Connected to the chip	N/A

4.1.1.3 EMI/EMC

The base cryptographic module has been tested to meet the EMI/EMC requirements specified by FCC Part 15, Subpart B, and Class B.

4.1.2 Transmission Protocol

The transmission protocols of the Hitachi MULTOS Smart Chip comply with ISO/IEC 7816-3 (half duplex character transmission protocols, T=0 and T=1).
The Hitachi MULTOS Smart Chip supports the Protocol and Parameter Selection to select a new protocol type or change the transmission baud rate.

4.2 LOGICAL INTERFACE DESCRIPTION

Once communication is established between the external device like a reader and the platform. The I/O ports of the platform provide the following logical interfaces:

Data In: I/O Pin (Bi-directional)
Data Out: I/O Pin (Bi-directional)
Status Out: I/O Pin (Bi-directional)
Control In: I/O Pin (Bi-directional), CLK and RST Pins

Synchronization timing controls provided in part by way of the platform CLK clock input, manages the separation of these logical interfaces that use the same physical port.

Electrical (physical) contact and data link layer contact is established between the smart card chip and the external device by the external device issuing a RESET signal to the smart card chip which then responds with an "Answer To Reset (ATR)" related to the communication protocol. From this point on, the card functions as a "slave" processor to implement and respond to the external device's "master" commands. The card adheres to a well-defined set of state transitions. Within each state, a specific set of commands is accessible.

4.3 ISO/IEC 14443 RF INTERFACE (CONTACTLESS MODE)

4.3.1 Interface Physical Specifications

In the contactless mode, the cryptographic module uses only two electrical connections, LA and LB, to close the loop of an external antenna, as illustrated in the following picture. The two electrical connections LA and LB, used in contactless mode are physically different from the electrical connections used in contact mode.

The antenna is not within the cryptographic boundaries of the module.

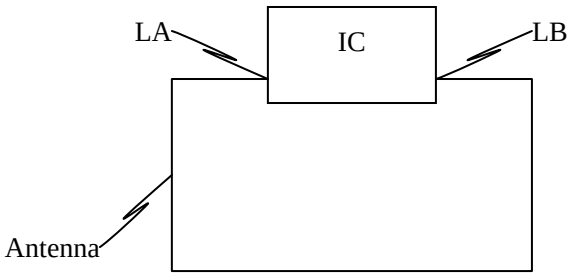

Figure 3: Example of connection of the cryptographic module to the antenna for the contactless mode

4.3.2 Interface Electrical Specifications

Power and data are transmitted to the module from the antenna using a modulation signal at 13.56 MHz. The proximity communication device like as reader produces an RF field that couples to the Chip Assembly (Hitachi MULTOS Smart Chip) to transfer power. Data communication from external device to chip is achieved through a modulation of the RF field, using amplitude shift keying (ASK) type of modulation.

During contactless communication, IC chip generates all power and clock signal from RF signal.

RF signal and power interface are fully compliant with ISO/IEC 14443 part 2: radio frequency power and signal interface for contactless integrated circuit cards – proximity cards.

A transmission protocol that defines data exchange between reader and cards are fully compliant with ISO/IEC 14443 part 4.

Table 3 –Functional Specifications of Chip Contacts in Contactless mode

Contactless	**FIPS 140 Logical Interface**
LA/LB	Data Input
LA/LB	Data Output
LA/LB	Control Input
LA/LB	Status Output
LA/LB	Power Interface

4.3.3 Transmission protocol

Communications with the Hitachi MULTOS Smart Chip in contactless mode is based on a fully standardized (ISO/IEC 14443), half-duplex transmission protocol, called T=CL.

5. MODE OF OPERATION

The following specific actions are required on the part of the Card Application Provider along with a restriction within the module usage environment to ensure the module operates in this mode.

1. The Card Application Provider must confirm all card functions to require a PIN for all Sign operations.
2. The Card Application Provider must set the PIN Policies for the Card Holder to have a minimum length of eight bytes.
3. The Card Application Provider must set the incorrect PIN counter to ten failed attempts before locking the card.
4. For key zeroization purposes, Card Application Provider may reload the Card Application to overwrite all data with MULTOS scheme.

6. MODULE CRYPTOGRAPHIC FUNCTIONS

The purpose of this cryptographic module is to provide FIPS approved cryptographic services with PIV function. Cryptographic keys and PINs represent the roles involved in controlling the card. A variety of FIPS 140-2 validated algorithms are used in this cryptographic module to provide cryptographic services in FIPS mode. These include:

- Triple-DES (192bit keys Decryption and encryption of challenge data for authentication) Certificate #429
- Deterministic RNG (used for generating random numbers) Certificate #186

The module also has non-approved functions that are not to be used in FIPS mode of operation: These include:

- RSA PKCS#1 (1024bit keys encryption of challenge data for authentication)
- Non-Deterministic RNG (used for generating seeds)

Table 4 – Keys used

Key Description	Key Type	Generation	Storage
Card Application Administrator Key	Triple DES 192	Loaded as part of the initialization process	Stored in EEPROM
Application Authentication Key	RSA 1024	Generated automatically as specified in ANSI X9.31 using PRNG.	Stored in EEPROM
RNG Key	Triple DES	Recreated from stored seed	Stored in RAM

6.1 RANDOM NUMBER GENERATORS

The cryptographic module offers the services of a FIPS 140-2 approved DRNG (Deterministic Random Number Generator) which is specified by ANSI X9.31 with 2 key Triple DES.

The cryptographic module also offers the services of a hardware based NDRNG (Non Deterministic Random Number Generator), which is used to generate a seed to feed the DRNG.

7. SELF TESTS

7.1 POWER-UP SELF TESTS

"Personal Identity Verification Application on Hitachi MULTOS Smart Chip" performs

the following self-tests to ensure that the module works properly.

The power-up self test include:

• EEPROM integrity check using EDC greater than 16 bit checksum
• Cryptographic Known Answer Tests for
    O Triple-DES decryption and encryption
    O RNG KAT
    O RSA Encryption KAT

The conditional tests include:

    O Continuous Random Number Generator Test

7.2 SELF-TEST EXECUTION

After “Personal Identity Verification Application on Hitachi MULTOS Smart Chip” is powered up and before executing any APDU commands received over either the contact or contactless interface, the module enters the self-test state and performs all of the cryptographic algorithm and software integrity self-tests as specified in FIPS 140-2 standard. These tests are conducted automatically as part of the normal functions of the cryptographic module. They do not require any additional operator intervention, or application specific functions.

Power-up self-tests are executed on reception of the first APDU command, after the module reset. The cryptographic module start-up process has been designed in such a way that it cannot be bypassed. This enforces the execution of the self-tests before allowing any use and administration of the module, thus guaranteeing a secure execution of the module cryptographic services.

If these self-tests are passed successfully, the cryptographic module returns the status words relating to the requested APDU command via the status interface and incoming APDUs are processed.

If any of the FIPS 140-2 power-up self-tests fail, the cryptographic module enters a mute state in which no response data is returned for the initial APDU. Further APDUs are not processed. After a reset, the cryptographic module will re-attempt the FIPS 140-2 power-up self-tests upon receipt of the first APDU.

Power-up self-tests can be executed on demand by issuing the SELECT command. All data output via the output interface are inhibited while any power-up and conditional self-test is running.

8. ROLES & SERVICES

8.1 ROLES

The “Personal Identity Verification Application on Hitachi MULTOS Smart Chip” module performs identity-based authentication using PIN and cryptographic key. A unique index value is associated with the PIN or the cryptographic key to uniquely identify the off-card entity performing the authentication.

The module defines three distinct roles that are supported by the on-card cryptographic system: the Card Application Administrator, Card Holder, and an unauthenticated role.

- Card Application Administrator is a role authenticated by demonstrating knowledge of Application Administrator Key (PIV Application Key 0x9B).
- Card Holder is a User role authenticated by knowledge of Card Holder Card Application PIN.
- Unauthenticated role is a role which may view status information or determine whether a smart card can communicate with a terminal application.

The module ensures the authentication of off-card entities (Card Application Administrator, and Card Holder) and provides them with cryptographic services according to their role.

Table 5 – Roles and Authentication

Role	Type of Authentication	Authentication Data
Card Application Administrator	Identity Based	Triple DES Key
Card Holder User	Identity Based	Card ID + 8 Digit PIN
Unauthenticated Role	None	None.

8.1.1 CARD APPLICATION ADMINISTRATOR

The Card Application Administrator authenticates his role on the card by

demonstrating to the PIV application that he possesses the knowledge of the Card Application Administration Key within the Card. The authentication process follows the Special Publication 800-73 specification. By successfully executing a series of commands, the Card Application sets the security status in the PIV Application;

Once established, authorization (on the card) to access information and services are granted by the PIV Application.

8.1.2 CARD HOLDER

The Card Holder (User) is responsible for ensuring the ownership of his card and for not communicating his PIN. The User is authenticated by verification of a PIN (Card Holder Card Application PIN for card application) that the User has selected at issuance and a Key Reference. PIN verification is provided using VERIFY COMMAND.

8.2 MODULE SERVICES (PER ROLE)

8.2.1 CARD APPLICATION ADMINISTRATOR

A Card Application Administrator authenticates his role to issue commands by proving knowledge of a key and using the key to successful. These commands include:

GET DATA: Retrieves the data contents of a single data object whose tag is given in the data field.

RESET RETRY COUNTER**:** Resets the retry counter of the key reference to its initial value and changes the reference data associated with the key reference. The command enables recovery of the PIN card application in the case that the cardholder has forgotten a PIV Card Application PIN.

Only retry counters associated with key references specific to the PIV Card Application; i.e. local key references, shall be reset by the PIV Card Application RESET RETRY COUNTER command.

GENERAL AUTHENTICATE (External): performs a cryptographic operation such as an authentication protocol using the data provided in the data field of the command and returns the result of the cryptographic operation in the response data field.

GENERATE ASYMMETRIC KEY PAIR: initiates the generation and storing in the card of the reference data of an asymmetric key pair, i.e., a public key and a private key. The public key of the generated key pair is returned as the response to the command. If there is reference data currently associated with the key reference, it is replaced in full by the generated data.

PUT DATA: The PUT DATA card command completely replaces the data content of a

single data object in the PIV Card Application with new content.
SELECT: sets the currently selected application. The PIV Card Application shall be selected by providing its application identifier
GENERAL AUTHENTICATE (Internal): used to authenticate the card or a card application to the client-application using symmetric or asymmetric keys. This is a non FIPS approved service.
GET MANUFACTURER DATA: retrieves the unique identification number of the card.
GET MULTOS DATA: retrieves information regarding the MULTOS OS.

8.2.2 CARD HOLDER SERVICES

The following commands are available to the Card Holder:

GET DATA (All Data): Retrieves the data contents of a single data object whose tag is given in the data field.
CHANGE REFERENCE DATA: initiates the comparison of the verification data with the current value of the reference data and if this comparison is successful replaces the reference data with new reference data. Only reference data associated with key references specific to the PIV Card Application can be changed by this PIV Card Application command. Only reference data associated with key references specific to the PIV Card Application; i.e. local key references, shall be changed by the PIV Card Application CHANGE REFERENCE DATA command.
GENERAL AUTHENTICATE: used to authenticate the card or a card application to the client-application using symmetric or asymmetric keys. This is a non FIPS approved service.
SELECT: sets the currently selected application. The PIV Card Application shall be selected by providing its application identifier.
VERIFY: initiates the comparison in the card of the reference data indicated by the key reference with authentication data in the data field of the command.
Only key references specific to the PIV Card Application; i.e. local key references, shall be verified by the PIV Card Application VERIFY command.
GET MANUFACTURER DATA: retrieves the unique identification number of the card.
GET MULTOS DATA: retrieves information regarding the MULTOS OS.

8.2.3 UNAUTHENTICATED SERVICES (NO ROLE)

The following commands are available without requiring authentication:

SELECT: sets the currently selected application. The PIV Card Application shall be selected by providing its application identifier.

GET DATA (subset of Data): Retrieves the data contents of a single data object whose tag is given in the data field.

GET MANUFACTURER DATA: retrieves the unique identification number of the card.

GET MULTOS DATA: retrieves information regarding the MULTOS OS.

GENERAL AUTHENTICATE (Internal): used to authenticate the card or a card application to the client-application using symmetric or asymmetric keys. This is a non FIPS approved service.

Table 6 – Roles and Services

Role	Authorized Services	Cryptographic Keys and CSPs	Type(s) of Access
Administrator	GET DATA (contact/contactless)	None	Read
	RESET RETRY COUNTER (contact)	PUK	Write
	GENERAL AUTHENTICATE (External) (contact)	Triple DES	Execute
	GENERATE ASYMMETRIC KEY PAIR (contact)	RSA Public/Private	Execute
	PUT DATA (contact)	None	Write
	SELECT (contact/contactless)	None	Execute
	GET MANUFACTURER DATA (contact)	None	Read
	GET MULTOS DATA (contact)	None	Read
	GENERAL AUTHENTICATE (Internal) (Non-Approved) (contact/contactless)	RSA, Triple-DES	Execute
User	GET DATA (contact/contactless)	None	Read
	CHANGE REFERENCE DATA (contact)	PIN	Write
	GENERAL AUTHENTICATE (Internal) (Non-Approved) (contact/contactless)	RSA, Triple-DES	Execute
	SELECT(contact/contactless)	None	Execute
	GET MANUFACTURER DATA (contact)	None	Read

	GET MULTOS DATA (contact)	None	Read
	VERIFY (contact)	PIN	Execute
Unauthenticated	SELECT (contact/contactless)	None	Execute
	GET DATA (contact/contactless)	None	Read
	GET MANUFACTURER DATA (contact)	None	Read
	GET MULTOS DATA (contact)	None	Read
	GENERAL AUTHENTICATE (Internal) (Non-Approved) (contact/contactless)	RSA, Triple-DES	Execute

9 CRITICAL SECURITY PARAMETERS

9.1 ASYMMETRIC CRYPTOGRAPHIC KEYS

The “Personal Identity Verification Application on Hitachi MULTOS Smart Chip” module includes the following keys:

- Authentication Key, Key Reference Value is 9A 9C 9D, used for the authenticate Card Application from terminal. Module detail is defined in Special Publication 800-73 section 5.5.

The device using the GENERATE ASYMMETRIC KEY PAIR COMMAND generates the RSA key pair.

9.2 SYMMETRIC CRYPTOGRAPHIC KEYS

The “Personal Identity Verification Application on Hitachi MULTOS Smart Chip module also includes the following key:

- Card Application Administrator Key is a triple DES key, Key Reference Value is 0x9B, used for the authenticate Card Application Administrator from Card Application. Module detail is defined in Special Publication 800-73 section 5.5.

This key is preinstalled in this card at the issuing facility.

9.3 OTHER CSPs

The “Personal Identity Verification Application on Hitachi MULTOS Smart Chip module includes one Personal Identification Number [PIN] managed by the Access Control Application):

- A Card Holder Card Application PIN used by the Card Holder to authenticate to a

Card Application. The PIN length is 8 Bytes. This PIN may be used to authenticate the Card Holder to the card. That is, by successfully entering a PIN sequence, a Card Holder can prove knowledge of a shared secret (the PIN) and thereby authenticate himself to the card. The CHANGE REFERENCE DATA COMMAND is available to the Card Holder to change the PIN.

- RNG Key is a triple DES key used in the random number generation process.
- A PIN Unblocking Key (PUK) is not an encryption key but a PIN used to unlock a blocked PIN. This is used as part of the RESET RETRY COUNTER command.

10 SECURITY RULES

10.1 IDENTIFICATION & AUTHENTICATION SECURITY RULES

The module implements specific methods for authenticating the different roles defined Special Publication 800-73. The implementation consists of the binding of an Identity-based Access Control Rule to each service that requires a role.

10.1.1 CARD HOLDER IDENTIFICATION AND AUTHENTICATION

Proving knowledge of the Card Holder Card Application PIN authenticates the Card Holder.

10.1.2 CARD APPLICATION ADMINISTRATOR IDENTIFICATION AND AUTHENTICATION

The Card Application Administrator must prove knowledge of the Application Administrator Key to authenticate his role.

10.2 PHYSICAL SECURITY RULES

The physical security of the “Personal Identity Verification Application on Hitachi MULTOS Smart Chip” 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 card is in possession of the Card Administrator until it is ultimately issued to the end user.

10.3 KEY MANAGEMENT SECURITY POLICY

10.3.1 CRYPTOGRAPHIC KEY GENERATION

Triple DES key is preinstalled in this card at issuing. This key is retained securely within the Data Model Container. No command can read it.

RSA key pairs may be generated using the GENERATE ASYMMETRIC KEY PAIR COMMAND function along with a key Reference Value. The public key is returned from the function and may be used externally from the module by being included on a digital certificate establishing the relationship between the public-key and the role of the Card Holder. These private-keys are retained securely within the Data Model Container.

10.3.2 CRYPTOGRAPHIC KEY STORAGE

All secret and private keys are structured to contain the following parameters:

- Key Reference value
- Algorithm Identifier

10.3.3 CRYPTOGRAPHIC KEY DESTRUCTION

The module destroys secret and private cryptographic keys and CSP's by using a GENERATE ASYMMETRIC KEY PAIR COMMAND with a key length value of the key component set to zero.

10.4 STRENGTH OF AUTHENTICATION

10.4.1 Card Application Administrator key

The length of the triple-DES key used for the authentication of the card application administrator is 192 bytes. This means that there are 2^{192} possible keys, which far exceeds the 1 in a million test.

10.4.2 PIN

The length of the Card Holder Card Application PIN and PUK is 8 Bytes. PIN and PUK may contain any keyboard characters including Shift-number combinations. For example if each byte of an 8 byte PIN were an alphanumeric character (a-z, A-Z, 0-9), it would yield a minimum of 62^8 possible PIN and PUK. This far exceeds the 1 in a million test.

An 8-bit counter internal to the Access Control program limits the number of failed PIN attempts an attacker could perform by blocking the card if the counter limit (10 attempts set in this mode) is exceeded.

11 SETUP AND INITIALIZATION PROCEDURES

11.1 Procedures Required for Setup and Initialization

The procedures necessary to put the Personal Identity Verification Application on Hitachi Multon Smart Card in FIPS mode include:

1. Load Mandatory Data Objects on the smart card using the PUT DATA command. Mandatory Data Objects are for interoperable use of PIV application. These objects are described at Special Publication 800-73 specification, table 6.
2. The Crypto-Officer must generate an Asymmetric Key Pair using the GENERATE ASYMMETRIC KEYPAIR command.
3. The Crypto-Officer must set the PIN Policies for the Card Holder to have a minimum length of 8 bytes.
4. The Administrator must set the PIN counter to ten failed attempts before blocking the card.
5. The User must change the default PIN using the CHANGE REFERENCE DATA command.

12 SECURITY POLICY CHECK LIST TABLES

12.1 ROLES & REQUIRED AUTHENTICATION

Table 7 - Roles and Required Authentication

Role	Type of Authentication	Authentication Data
Card Application Administrator	Triple-DES authentication	Triple-DES key (Challenge response)
Card Holder	PIN	Card Holder PIN

12.2 STRENGTH OF AUTHENTICATION MECHANISMS

Table 8 - Strength of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Triple-DES authentication	High (Far exceeds the 1 in a million test)
PIN	High (Far exceeds the 1 in a million test)