MIIKOO

FIPS 140-2 Cryptographic Module

Non-Proprietary Security Policy

Pierson Capital Technology LLC **Oct 20th, 2011**

Revision: 1.1

Status: Public release

Table of Contents

Change Log

Name	Date	Version	Remarks
Likely Lee	04/06/2010	0.1	Document created.
Likely Lee	15/06/2010	0.2	Modify according to suggestions. Add Glossary, Ports sections
Likely Lee	25/06/2010	0.3	Add Data flow. Modify FSM
Likely Lee	11/07/2010	0.4	Modify the block diagram, ports & interfaces, FSM
Likely Lee	13/07/2010	0.5	Rearrange the document
Likely Lee	23/07/2010	0.6	Modify according to the RA summary
Likely Lee	26/07/2010	0.7	Add Diffie-Hellman as key establishment
Likely Lee	27/08/2010	0.8	Modify the key management part
Likely Lee	02/09/2010	0.8	Add a statement to FSM and module description
Likely Lee	10/09/2010	0.8	Modify the declaration in Rules of Operation
Likely Lee	29/10/2010	0.9	Modify the firmware version and FSM
Likely Lee	28/04/2011	0.9	Modify according to Alejandro's Comments
Likely Lee	13/05/2011	0.9	Modify the Authentication and Identification part
Likely Lee	17/05/2011	0.9	Modify according to Alejandro's Comments
Frank	18/05/2011	1.0	Correct English problems
Likely Lee	27/05/2011	1.0	Modify the PIN authentication and PIN length
Likely Lee	02/06/2011	1.0	Modify the module components and reference
Likely Lee	03/06/2011	1.0	Document published
Likely Lee	01/09/2011	1.1	Modify according to CMVP's comments
Likely Lee	19/09/2011	1.1	Update reference 12
Likely Lee	20/10/2011	1.1	Update the page footer, update module description

Introduction

The objective of MIIKOO System is to offer highly secure access for sensitive applications such as e-banking, e-purse cash downloads, secure e-commerce and Dynamic PIN (Personal Identification Number) for existing POS (Point-of-Sale) and ATM (Automatic Teller Machine) terminals.

MIIKOO device (hereinafter referred to as the cryptographic module or the module) combines fingerprint recognition and additional cryptography capabilities to generate Dynamic PINs. It is compatible with all types of smart IC, magnetic stripe or contact-less cards by seamlessly providing an added biometric triggering of a dynamic PIN over the existing financial transaction network.

Biometrics are never transmitted over the network, authentication to the backend server is based on the dynamic PIN generated by the module. A high profile fingerprint sensor is implemented on the module to provide the level of security the financial industry requires. The sensor is provided by AuthenTec and the fingerprint matching algorithm is provided by Synochip.

Figure 1: Module Overview

For Traditional Banking

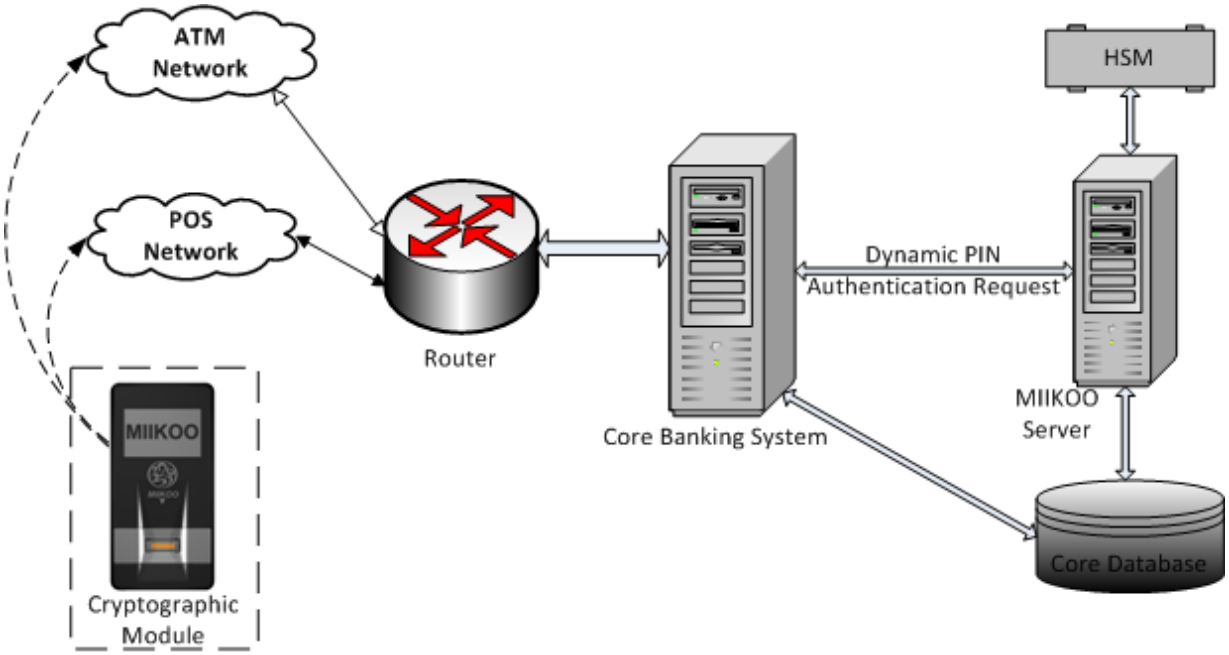

Figure 2: Traditional Banking Systems

When the module is used for traditional banking such as on ATMs or POSes, the user inserts the bank card into the ATM or swipes the card on the POS, then swipes his registered fingerprint on the module; if the fingerprint captured matches the one stored on the module, the module will calculate the dynamic PIN and displays it on the LCD screen. The user enters this dynamic PIN on the keypad of the ATM or POS and the transaction is done. This dynamic PIN is only valid for 1 minute.

The module has a non-replaceable Li-ion battery which can be recharged through the USB port. Once fully charged, the module can be used for at least 3 months. Even if the battery power is not enough for normal operation, it can still keep the real time clock running for 3 years.

For Online Banking

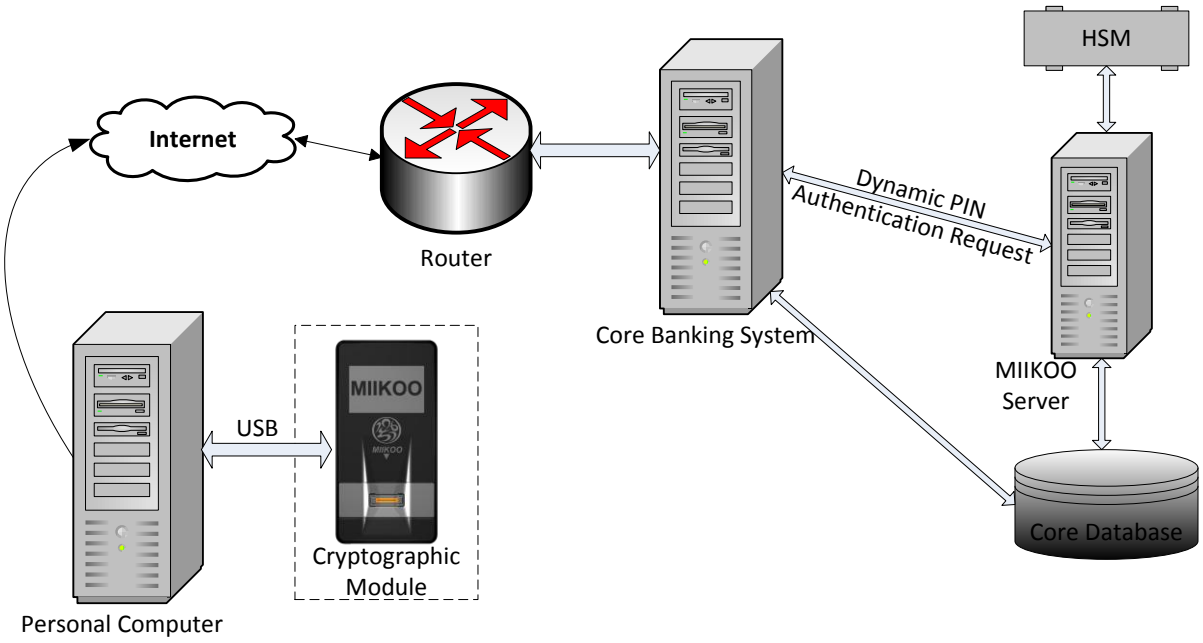

Figure 3: Online Banking System

When the module is used for online banking, the user needs to connect the module to a GPC via a mini USB cable; open the e-banking login page or e-commerce payment page, and swipe his registered finger on the module; if a match is acquired, the user can check his e-banking account or finish the payment in process. The e-banking and e-commerce are functioning through a web browser on the host GPC that the CM is connected to. The CM provides the necessary login credential on the behalf of user to authenticate the user against the communicating e-bank or the e-commerce provider.

Other

The module can also be used for signing documents. The user needs to connect the module to a GPC via the mini USB cable, and then he can use the application such as Microsoft Outlook, Microsoft Word or Adobe Acrobat to sign his documents or emails by simply swiping the registered finger. The documentation signing function is not solely performed by the CM. Rather it is a function supported by applications such as Microsoft Outlook, Microsoft Word or Adobe Acrobat that run on the host GPC. These applications send the hash values of the documents to be signed to the CM via GPC. The CM sends back to them the encrypted hash values under the RSA private key stored on the CM.

This document focuses on the features and security policy provided by the module, and describes how the module is designed to meet FIPS 140-2 compliance.

Cryptographic Module Specification

Module Description

The module provides end to end encryption for sensitive applications such as e-banking, e-trade, e-commerce and Dynamic PIN for existing POSes and ATMs. The dynamic PIN is calculated according to an HMAC-based One Time Password algorithm and is hence an OTP value that is valid only for one minute. The module combines fingerprint recognition and OTP generation with additional cryptography capabilities, tamper resistant casing and a display to ensure high security access. "Dynamic PIN" and "OTP" are used interchangeably hereafter in this document.

During the manufacturing process, the module is loaded with the factory version firmware. This firmware is only used for testing purpose, including basic communication functions and hard-coded handshake key. After packaging, the module will be shipped to the clients. When the user wants to use this service, he needs to go to the bank to subscribe. The bank's customer service officer will plug two modules into the GPC, one is his own admin module and another one is the user's module. Then the customer service officer can use his admin module to login to the administration server and update the factory version firmware with the FIPS 140-2 certified version firmware on the user module. The certified version firmware disables the firmware updating functionality. The firmware on the module cannot be further updated. Once the certified version firmware is loaded into the user module, the customer service officer must initialize it. The File key is generated in the initialization stage and the TSK, handshake key and Decrypt TSK key are transferred to the module from the bank's server during the initialization stage. The customer service officer will ask the user to input the information and register the fingerprints into the module. During the registration stage, TMK, TPK, DSK and PVK are generated and transferred to the module from the bank's server.

Module Components

The following table lists the module components:

Type	Name	Release
Hardware	MIIKOO Device FIPS 140-2 Cryptographic Module	D4
Firmware	MIIKOO Device Bootstrap	v3.1
	MIIKOO Device Application	006262
	MIIKOO Device Algorithm Library FIPS 140-2 Cryptographic Algorithm	v2.1

Security Policy	MIIKOO Device FIPS 140-2 Cryptographic Module Security Policy	1.0
Manual	MIIKOO Device User Manual	1.0
	MIIKOO Account Registration	1.0
	MIIKOO Device System Initialization	1.1
Design Documentation	MIIKOO Device D4 Specification	1.0
	MIIKOO Device Applet Handshake	1.0
	MIIKOO Device Applet Communication Protocol	1.0
	MIIKOO Key Management	1.0
	MIIKOO Module Services	1.0
	MIIKOO Main Component List	1.0
	MIIKOO Configuration List	1.0

Table 1: Module Component List

Module Block Diagram

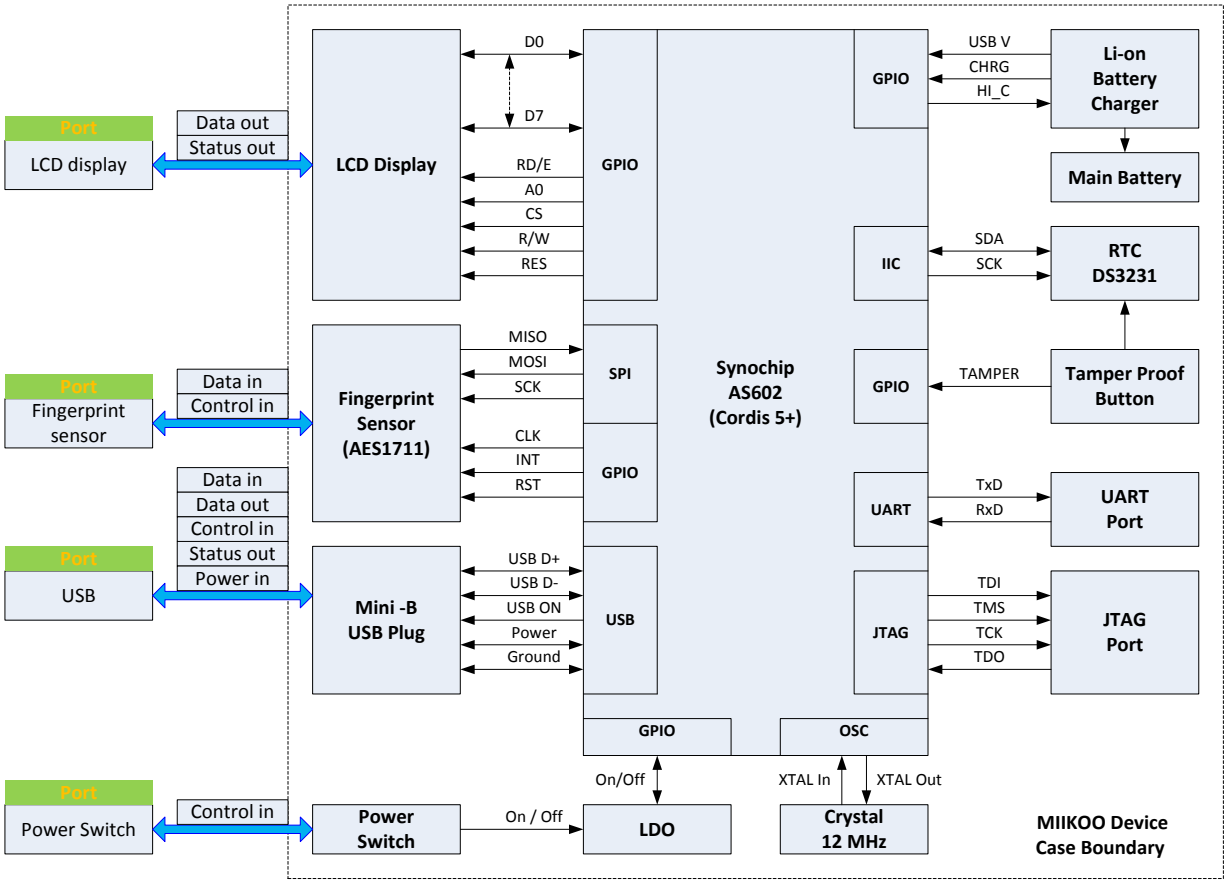

Figure 4: Block diagram of the cryptographic module

The module consists of a micro processor unit, a fingerprint sensor, an LCD display, a real time clock, a battery and relevant circuits. The module can be powered by either the internal rechargeable Li-ion battery or an external power supply through the USB port. The dimension of the module is: 70 x 35 x 10 mm.

The micro processor unit AS602 works at 120MHz. It provides a set of high performance peripherals including Cordis 5+ DSP core, 128 KB SRAM, 64KB ROM, 4K bits OTP memory, 1MB Flash and USB port.

The module provides 4 cross boundary ports: LCD display, fingerprint sensor, USB port and power switch.

Another two ports (UART and JTAG) are provided for manufacturing and debugging purposes only. They are sealed with epoxy and cannot be accessed by end users of the module.

The module interacts through the USB port with a JAVA applet that runs on many operating systems including Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows Vista, Microsoft Windows 7, Linux and Mac OS X, and also many internet browsers including Internet Explorer, Firefox, Google Chrome and Safari. The communication between the JAVA applet and the module is encrypted. The module and the JAVA applet use the Diffie-Hellman protocol to generate the communication encryption key, and then use this key to encrypt all messages by means of the Triple-DES algorithm. The USB port is also used to charge/re-charge the battery.

The micro processor unit captures fingerprint images from the fingerprint sensor, and generates fingerprint templates or performs matching with templates stored in flash memory.

The LCD displays the dynamic PIN, the battery and connection icons, the account number, the FIPS mode indicator and error messages.

The power button is only used to switch on the module.

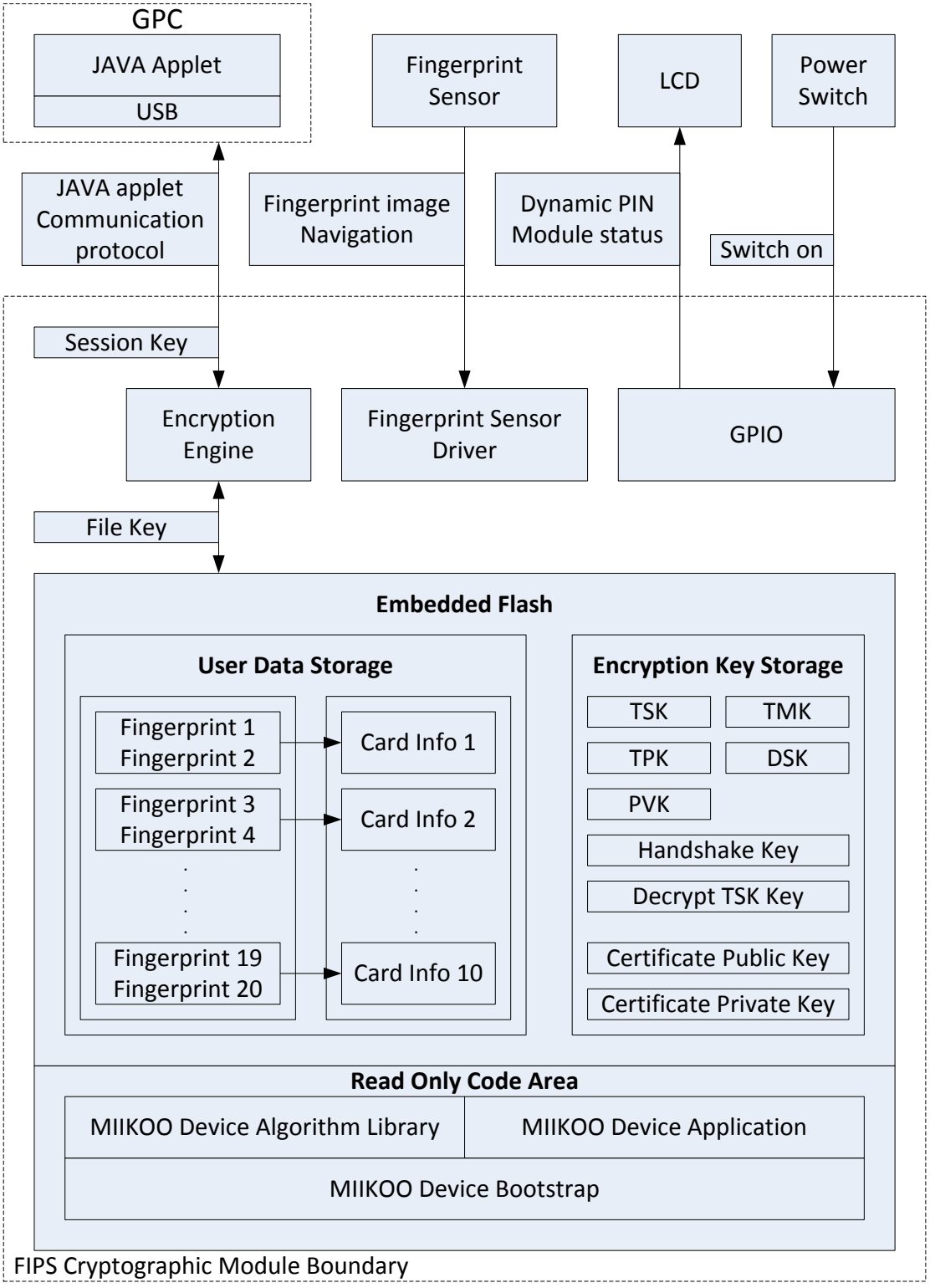

Figure 5: Data flow of the cryptographic module

Algorithm List

The module provides the Algorithm Library together with the firmware application. The Algorithm Library supports the following FIPS-approved and non FIPS-approved algorithms:

FIPS Approved Algorithms				
Type	**Algorithm**	**Specification**	**Validation Certificate**	**Use**
Hash Functions	SHA-256	FIPS 180-3	1351	hashing integrity check
	HMAC based on SHA-256	FIPS 198	884	hashing
Cipher Functions	Triple-DES-ECB	NIST SP 800-38A	1004	encrypt / decrypt operations
	Triple-DES-CBC	NIST SP 800-38A	1004	encrypt / decrypt operations
Public Key	Signature Generation based on PKCS#1 v1.5 with 2048 bits	FIPS 186-2 RSASSA-PSS RSASSA-PKCS1	737	generate signature operations
	Signature Verification based on PKCS#1 v1.5 with 2048 bits	FIPS 186-2 RSASSA-PSS RSASSA-PKCS1	737	verify operations
	Key Generation Based on X9.31 with 2048 bits	ANSI X9.31	737	key generation
Random Number Generator	DRBG800-90 SHA-256 based DRBG	NIST SP 800-90	63	random number generation

Table 2: FIPS approved algorithms

Non FIPS Approved Algorithms			
Type	**Algorithm**	**Specification**	**Use**
Key establishment	Diffie-Hellman With 2048 bits	RFC2631	key establishment

Table 3: Non FIPS approved algorithms

FIPS 140-2 Validation Level

The module was tested and certified to the following FIPS 140-2 defined levels:

Sections	Security Levels			
	1	2	3	4
Cryptographic Module Specification			✓	
Cryptographic Module Ports and Interfaces			✓	
Roles, Services and Authentication			✓	
Finite State Model			✓	
Physical Security			✓	
Operational Environment			N/A	
Cryptographic Key Management			✓	
EMI/EMC			✓	
Self-Tests			✓	
Design Assurance			✓	
Mitigation of Other Attacks			N/A	
Cryptographic Security Policy			✓	
Overall Security Level:	**3**			

Table 4: FIPS validation level

Cryptographic Module Ports and Interfaces

The cryptographic module is classified as a "Multi-chip Standalone Cryptographic Module" for FIPS 140-2 purposes. The module consists of hardware which connects to a General Purpose Computer (GPC) through USB port, and all the data stored inside the module can only be accessed through the USB port. The hardware includes the micro processor unit, fingerprint sensor, high accuracy real time clock, LCD, Li-ion battery and peripherals such as voltage monitor and battery charger.

Ports

The physical ports that cross the case boundary are the following: USB, LCD display, fingerprint sensor and power switch.

USB

The USB port is used to connect to the host computer via a Mini-B USB cable, compliant with the Universal Serial Bus Specification Revision 2.0. The device type is defined as Human Interface Device (HID). All data, commands and status are transferred only through this port. Additionally, the module can be powered on from this port.

LCD display

The LCD display port is used to show the dynamic PIN and the module status. No CSPs can be accessed via this port.

Fingerprint sensor

The Fingerprint sensor port is used to capture fingerprint images and do the LCD display navigation. No CSPs can be accessed via this port.

Power switch

The Power switch port is used to switch on the module only. No CSPs can be accessed via this port.

Interfaces

The logical cryptographic interface is the encrypted communication protocol with Diffie-Hellman key exchange. The protocol is used by the referencing JAVA applet running in the GPC to connect and control the module.

The physical ports provided by the module are mapped onto the FIPS 140-2 logical interfaces: data input, data output, control input, status output and power input. Each of the FIPS 140-2 logical interfaces relates to the module's callable interface, as follows:

- Data input: input parameters to all functions defined in Reference 9 that accept input from Admin or User entities. USB and Fingerprint sensor ports are mapped to data input interfaces.
- Data output: output parameters from all functions defined in Reference 9 that return data as arguments or return values to Admin or User entities. USB and LCD display ports are mapped to data output interface.
- Control input: all commands input into the module by Admin and User entities. USB, Fingerprint sensor and Power switch ports are mapped to the control input interfaces.
- Status output: status information returned from the module to Admin or User entities. USB and LCD display ports are mapped to status output interface.
- Power input: external power input into the module by Admin and User entities. USB port is mapped to the power input interfaces.

The complete list of APIs is documented in Reference 9.

Roles, Services and Authentication

Roles

The Super Admin, Admin, User, PKI Admin and PKI User roles can access services implemented in the module.

Role in FIPS 140-2 term	Role defined in the CM	Authentication Method	Note
Crypto officer	Super Admin	N/A	Super Admin is a specific role only used for generating the first Admin role after the whole MIIKOO system setup deployment has been finished. The Super Admin role can only be used once in the whole MIIKOO system lifecycle. It is only intended for devices used for administering the MIKOO system, not for the end user.
Crypto officer	Admin	Fingerprint Account number	The Admin role is used to manage the entire MIIKOO system including the MIIKOO CM throughout its operational lifecycle.
User	User	Device PIN Fingerprint Account number	The User role is the regular user of the module which can make use of some of the OTP functions.
Crypto officer	PKI Admin	PKI Admin PIN	The PKI Admin role is used to manage all the PKI functions.
User	PKI User	PKI User PIN Fingerprint	The PKI User role can make use of some of the PKI functions.

Table 5: Roles list

The module meets the FIPS 140-2 level 3 requirements for Roles and Services for Super Admin, Admin, User, PKI Admin and PKI User roles.

Services

The services provided by the module are listed in the following table. Detailed description of all the services can be found in Reference 18. All services except Self Test can be triggered from the server application through the USB port by using the commands defined in Reference 9.

Roles	Services	Critical Security Parameters	Algorithm	Authentication
Admin User	Get Account list	File key (decrypt account data from flash) Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	Yes (admin and normal account fingerprint)
Admin User	Set default account	File key (encryption account status into flash) Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	Yes (admin and normal account fingerprint)
Admin User	Deletion of account	File key (decrypt account data from flash and encrypt account data into flash) Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	Yes (admin and normal account fingerprint)
Admin User	Remote mode management	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	No
Admin User	Ping device	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	No
Admin User	Generate session key by Diffie-Hellman	Handshake key (encrypt sent out data and decrypt received data) File key (decrypt Handshake key from flash) Diffie-Hellman public key (received from host PC) Diffie-Hellman private key (generated by DRBG 800-90)	Triple-DES Diffie-Hellman DRBG 800-90	No
Admin User	Factory initialization	File key (encrypt TSK and device ID then restore into flash) decryption TSK key (decryption TSK) Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	No
Admin User	Change security level	File key (encrypt security level into flash)	Triple-DES	Yes (admin or normal

		Session key (encrypt sent out data and decrypt received data from USB)		account fingerprint)
Admin User	Factory reboot	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	No
Admin User	Get owner settings	File key (decrypt device information from flash) Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	No
Admin User	Set owner settings	File key (encrypt device information into flash) Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	Yes (admin or normal account fingerprint)
Admin User	Device Initialization	TSK (encryption device ID as authenticate key to get TMK) TMK (encryption TSK as authenticate key to get TPK) TPK (encryption TMK as authenticate key to get DSK) File key (encrypt TMK, TPK, DSK into flash, decryption TSK from flash) Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	No
Admin User	Account enrollment	File key (encrypt account information into flash) Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	Yes (Device will check the device PIN internal as authentication for the account enrollment. Enroll admin account or normal account must do the device PIN check first.)
Admin	Authentication	DSK (as HMAC key to Hash	Triple-DES	Yes

User		amount) PVK (encrypt account information) File key (decrypt DSK, PVK and account information from flash) Session key (encrypt sent out data and decrypt received data from USB)	HMAC-256	(admin or normal account fingerprint)
User	Dynamic PIN output	DSK (as HMAC key to Hash moving factor) PVK (encrypt device ID and hash value) File key (decrypt DSK, PVK and account information from flash), Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	Yes (normal account fingerprint)
Admin User	Real clock management	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	No
Admin User	Transaction log retrieval	File key (decrypt log data from flash) Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	Yes (admin and normal account fingerprint)
Admin User	Idle mode	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	No
Admin User	Fingerprint Authentication mode	File key (decrypt fingerprint image and account information) Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	Yes (admin or normal account fingerprint)
Admin User	Edit PIN mode	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	No
User	Offline PIN mode management	DSK (as HMAC key to Hash moving factor) PVK (encrypt device ID and hash value)	Triple-DES	Yes (normal account fingerprint)

		File key (decrypt DSK, PVK and account information from flash)		
Admin User	Clock show mode	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	No
Admin User	Fingerprint enrollment mode	TSK File key Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	No (Not require authentication, but to store the account fingerprint into device, device request at least have one account link to this account fingerprint. Otherwise account fingerprint will automatic delete by device)
Admin User	Fingerprint match mode	File key (encrypt fingerprint image into flash) Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	No
Admin User	Fingerprint Match mode management	File key (decrypt fingerprint image from flash) Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	No
Admin User	Select card mode	File key (decrypt account information from flash) Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	Yes (admin or normal account fingerprint)
Admin User	Device state report management	File key (decrypt device status from device) Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	No
Admin	Automatic change admin card number	File key (encrypt account data into flash) Session key (encrypt sent	Triple-DES	No There is no authentication

		out data and decrypt received data from USB)		requirement, but expect only using for active MIIKOO system start working by super admin role.
Admin User	Unblock device	TSK (decrypt receive device ID) File key (decrypt fingerprint image and encrypt unblock status data into flash) Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES	Yes (admin or normal account fingerprint)
Admin User	Self Test (including integrity, known answer and pair-wise consistency tests)	None	SHA-256 (using for integrity check) Triple-DES RSA DRBG800-90 HMAC-256	No
PKI Admin PKI User	PKI Get status	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES RSA	No
PKI Admin PKI User	PKI logout	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES RSA	No
PKI Admin PKI User	PKI Check in	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES RSA	Yes (PKI admin PIN or PKI user PIN)
PKI Admin PKI User	PKI Clear Device	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES RSA	Yes (PKI admin PIN or PKI user PIN or PKI fingerprint)
PKI Admin PKI User	PKI Fingerprint Match	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES RSA	No
PKI Admin PKI User	PKI Fingerprint Enroll	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES RSA	Yes (PKI admin PIN or PKI user PIN or PKI

				fingerprint)
PKI Admin PKI User	PKI Fingerprint Delete	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES RSA	Yes (PKI admin PIN or PKI user PIN or PKI fingerprint)
PKI Admin PKI User	PKI Get Fingerprint List	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES RSA	No
PKI Admin PKI User	PKI Open Container	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES RSA	No
PKI Admin PKI User	PKI Create Container Name	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES RSA	Yes (PKI admin PIN or PKI user PIN or PKI fingerprint)
PKI Admin PKI User	PKI Read Container Name	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES RSA	No
PKI Admin PKI User	PKI Delete Container	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES RSA	Yes (PKI admin PIN or PKI user PIN or PKI fingerprint)
PKI Admin PKI User	PKI Import Key-pair	Session key (encrypt sent out data and decrypt received data from USB) RSA key-pair (using for application encryption or decryption)	Triple-DES RSA	Yes (PKI admin PIN or PKI user PIN or PKI fingerprint)
PKI Admin PKI User	PKI Export public Key	Session key (encrypt sent out data and decrypt received data from USB) RSA public key (encryption data by public application)	Triple-DES RSA	No
PKI Admin PKI User	PKI Check certificate exist	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES RSA	No
PKI Admin PKI User	PKI Create random data	Session key (encrypt sent out data and decrypt received data from USB) Random data (generated by DRBG800-90)	Triple-DES DRBG 800-90	No
PKI Admin PKI User	PKI Generate RSA Key-pair	Session key (encrypt sent out data and decrypt	Triple-DES RSA	Yes (PKI admin PIN or

		received data from USB) RSA key-pair as certificate RSA key	DRBG 800-90	PKI user PIN or PKI fingerprint)
PKI Admin PKI User	PKI RSA encryption / decryption	Session key (encrypt sent out data and decrypt received data from USB) RSA public key (encrypt / decrypt data) RSA private key (encrypt / decrypt data)	Triple-DES RSA	Yes (PKI admin PIN or PKI user PIN or PKI fingerprint)
PKI Admin	PKI Format PIN	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES RSA	Yes (PKI admin PIN)
PKI Admin	PKI Unblock PIN	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES RSA	Yes (PKI admin PIN)
PKI Admin PKI User	PKI Set device Name	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES RSA	Yes (PKI admin PIN or PKI user PIN or PKI fingerprint)
PKI Admin PKI User	PKI Read Certificate	Session key (encrypt sent out data and decrypt received data from USB) Read certificate does not include RSA key pairs only certificate data. RSA public key use PKI Export public Key to export	Triple-DES RSA	No
PKI Admin PKI User	PKI Write Certificate	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES RSA	Yes (PKI admin PIN or PKI user PIN or PKI fingerprint) (write certification context not include public and private key, but without authenticate device can be write an invalid Certificate)
PKI Admin PKI User	PKI Delete Certificate	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES RSA	Yes (PKI admin PIN or PKI user PIN or PKI fingerprint)

PKI Admin PKI User	PKI Verify PIN	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES RSA	Yes (PKI admin PIN or PKI user PIN)
PKI Admin PKI User	PKI Get Retry Password Left Times	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES RSA	No
PKI Admin PKI User	PKI Change User Password	Session key (encrypt sent out data and decrypt received data from USB)	Triple-DES RSA	Yes (PKI admin PIN or PKI user PIN)

Table 6: Authorized Services

Authentication and identification

Authentication:

The module provides two different authentication types: PIN authentication and fingerprint authentication.

PIN authentication is used in account registration and PKI management. The minimum length of Device PIN is 6 numeric digits, and the minimum length of PKI User PIN and PKI Admin PIN is 8 alphanumeric digits. All the PINs supported by the module are listed in the following table:

PIN Name	Usage	Length
Device PIN	Used for user account registration	6 numeric digits
PKI User PIN	Used for PKI functions authentication	8 to 16 alphanumeric digits
PKI Admin PIN	Used for formatting and unblocking of PKI module	8 to 16 alphanumeric digits

Table 7: Authentication PIN used for module

Super Admin role is the first operator of the module, and normally he should be the manager of the security department, so there is no authentication for this role.

During system initialization the first admin account number is generated. Reference 13 describes the system installation and module initialization. The Admin role should use the Admin PIN to authenticate and then register his fingerprints. Once the Admin role is registered he can only use fingerprints to authenticate, and the Admin PIN is expired. This Admin PIN is authenticated in the server side, not in the module.

Every module has its own Device PIN. This PIN is given to the end user as a password envelop. The User role should use the Device PIN to authenticate and then register his fingerprint. Reference 16 describes how to register an account. The Device PIN is only used in

the first account registration, and after this all the other operations are authenticated by fingerprint and Device PIN is blocked.

When the module is configured as a PKI device in the first time, PKI Admin PIN and PKI User PIN are initialized as “11111111” and ”22222222”. PKI Admin role can use PKI Admin PIN to authenticate and then he should change the PKI Admin PIN and format the module immediately. And PKI User role should also be authenticated by the PKI User PIN and change it.

PKI Admin role will be asked to authenticate by PKI Admin PIN while performing PKI clear device, PKI format PIN (to change PKI Admin PIN) and PKI unblock PIN services. PKI Admin role can register fingerprint. After successful fingerprint registration, PKI Admin role can be authenticated by fingerprints.

PKI User role is required to authenticate by PKI User PIN while performing PKI Change User Password to change PKI User PIN. PKI User role can also register fingerprints. Before the PKI User role registers his fingerprint for the first time, he also needs to be authenticated by PKI User PIN. After successful fingerprint registration, PKI User role can be authenticated by fingerprints.

The fingerprint authentication is only done in the module. Fingerprint information of all roles is only stored in the module and in the same fashion, and can never be output.

Once the GPC closes the connection or the module is unplugged from the GPC, the authentication information will be erased. Next time when the GPC re-connects to the module, the module will require authentication again.

Identification:

When the module is configured as an OTP device, the identification is done by account number. The module is capable of storing up to ten account numbers. The admin account number and the user account number could co-exist in the same module. Two different fingerprints are required for each account number, one is the primary fingerprint and another is the backup. The GPC calls “Set owner settings” and “Account enrollment” to create a new account. Admin role and User role are determined by different account numbers. If the account number is predefined as an admin number then it is the Admin role. If the account number is a normal bank card number then it is the User role. Both the Admin role and the User role can use the OTP services after successful fingerprint authentication.

The module supports three different fingerprint authentication levels. In low level authentication, the user can authenticate with any of the registered fingerprints. In normal

level authentication, the user needs to authenticate with the primary registered fingerprint. Finally, in high level authentication, the user has to first authenticate with the primary fingerprint and then with the secondary fingerprint in the exact sequence they were registered.

It is also permitted for a user to register multiple account numbers using one primary fingerprint; before registering another account number, the user have to be correctly authenticated, and then user can follow the Reference 16 to register another account. If the module has multiple accounts registered, after authentication by swiping her finger, the user can tap on the sensor to select which account is going to be used for that particular session already authenticated. If the user wants to switch to another role, he needs to authenticate again.

When the module is configured as a PKI device the account identification is isolated from the OTP functions. The account numbers are not used in PKI functions. PKI Admin role and PKI User role can be identified by PKI Admin PIN and PKI User PIN.

The fingerprints registered in OTP mode cannot be used in PKI mode. PKI fingerprints are linked to PKI users only. The fingerprint matching level is the same in both OTP mode and PKI mode, but the fingerprint authentication level is different. In PKI mode user can register up to 5 different fingerprints and any one of them can be used for authentication.

Fingerprint matching level:

The FAR is 0.000001%. Reference 12 provides the fingerprint algorithm performance testing result. JAVA applet can call the service “Factory change security” to set the matching level of the fingerprint sensor. There are 5 different matching levels as shown in Table 8.

Matching level	Threshold for Authentication One of the two fingerprints	Threshold for Authentication First registered fingerprint	Threshold for Authentication Two fingerprints
0	50	45	45
1	55	50	45
2	60	55	50
3	65	60	55
4	70	65	60

Table 8: Fingerprint matching level

Threshold	FRR	FAR
45	2.145329%	0.000001%
50	2.733564%	0.000001%
55	3.010381%	0.000001%
60	3.460208%	0.000001%
65	3.979239%	0.000001%
70	4.671280%	0.000001%

Table 9: Threshold, FRR and FAR

FAR (False Acceptance Rate) is the probability that the system mistakenly matches an input fingerprint image to a fingerprint template saved in the database. It measures the percentage of invalid inputs being incorrectly accepted. FRR (False Rejection Rate) is the probability that the system fails to detect a match between the input fingerprint image and a fingerprint template saved in the database. It measures the percentage of valid inputs being incorrectly rejected.

The threshold value controls the degree of approximation between the input fingerprint image and a saved fingerprint template to be matched. Table 9 shows the correlation between the threshold value and the FRR and FAR. A higher threshold value means that a larger number of matching minutiae or feature points between the input fingerprint image and the saved fingerprint template is required. Therefore, a higher threshold value results in a higher FRR and a corresponding lower FAR.

Finite State Model

Figure 6 is a finite state diagram showing the states and transitions between states. At any point in time the module is in one and only one state. The state transitions are indicated by the arrows in the diagram.

Diagram

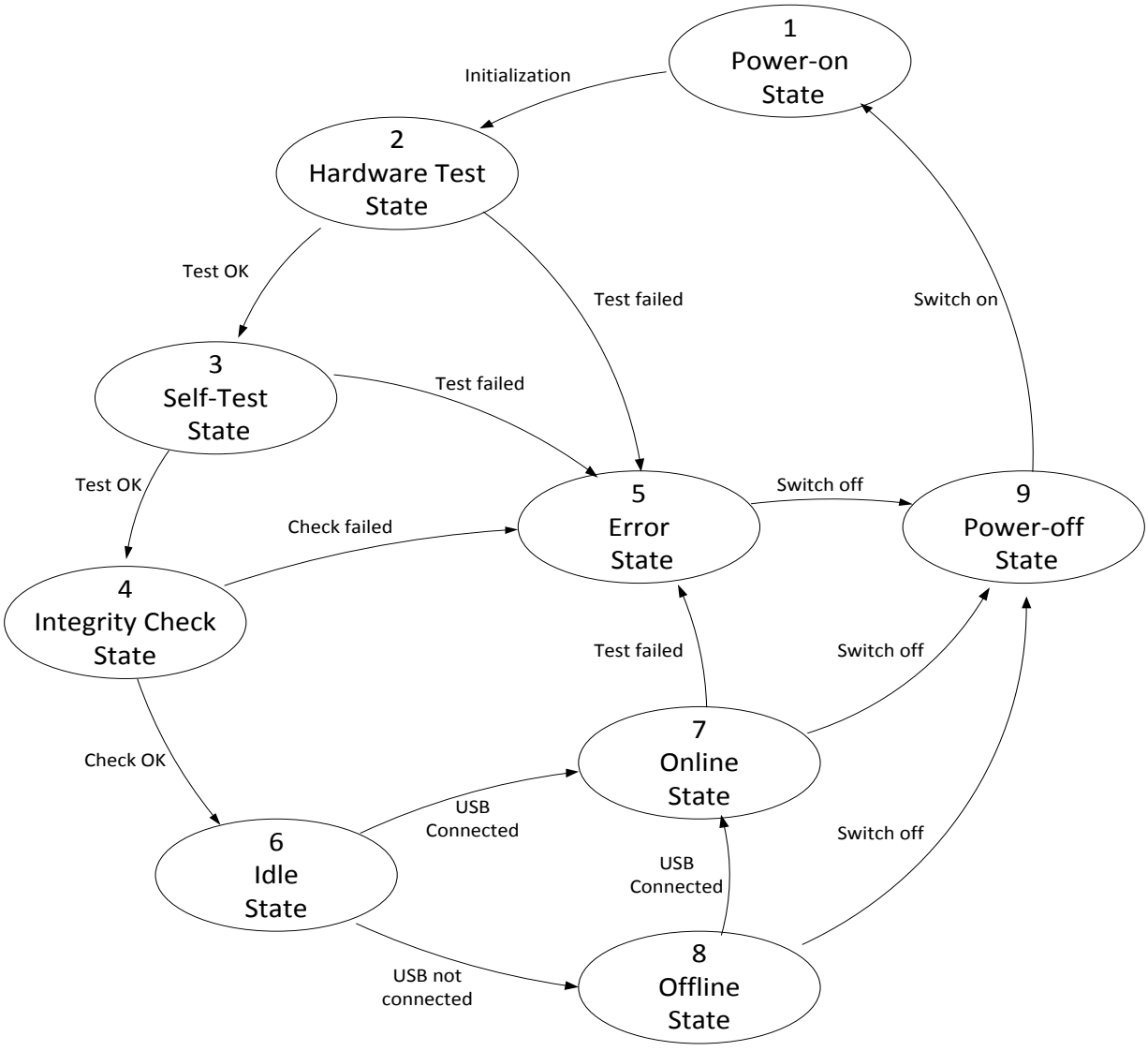

Figure 6: Finite State Machine Diagram

State Description

State 1: Power-on State

The cryptographic module transitions to the Power-on State when user presses the power button to switch on the system. Once the module finishes the initialization, it automatically transitions to the Hardware Test State.

State 2: Hardware Test State

The module checks the hardware components. The message “FIPS_INIT” will be shown on the LCD port. If the test is ok the module transitions to the Self-Test State. If the test fails, the module transitions to the Error State.

State 3: Self-Test State

The micro processor unit starts executing the startup codes and the FIPS Self-Test codes. If the module passes all the self tests it transitions to the Integrity Check State. If the self tests fail, the module transitions to the Error State.

When the module is in Self-Test State, all the requests sent from the USB port, fingerprint sensor port and power switch port will not be processed. Additionally, no message will be sent out to the USB port and LCD port.

State 4: Integrity Check State

The module checks the integrity of its firmware. If the integrity check is ok the module enters the FIPS mode and transitions to the Idle State. In FIPS mode, there is an “F” icon displayed at the upper left of the LCD. If the integrity check fails, the module transitions to Error State with all FIPS functions unavailable.

There is only one approved mode of operation; the unit successfully passing the power on self tests and integrity check causes the module to enter the approved mode.

State 5: Error State

Any error will cause the module transitions to this state. The reasons are shown in tables 10, 11, 12 and 13. In Error State, no FIPS-approved operation is allowed and all output except status output is inhibited. The module shows the ”FIPS ERR” messages to the LCD and 3 seconds later transitions to the Power-off State.

Type	Description
FP Init Failed	Fingerprint sensor initialization failed
Hard Fault	Other hardware fault

Table 10: Reasons for the Hardware Test

Type	Description
CRC32	KAT do not match
SHA256	KAT do not match
HMAC256	KAT do not match
TripleDES-CBC	KAT do not match
TripleDES-ECB	KAT do not match
DRBG	Second generated number equals to the first number
RSA	Key pair do not match

Table 11: Reasons for the Self Test

Type	Description
DRBG	Second generated number equals to the first number
RSA	Key pair do not match

Table 12: Reasons for the Conditional Test

Type	Description
Integrity	Integrity check value do not match

Table 13: Reasons for the Integrity Check

State 6: Idle State

The module enters this state after the power-on self-tests have executed successfully and the firmware integrity check is verified. Once the module enters the Idle State, it checks the card storage and USB connection status. If the USB port is connected to a GPC, the module transitions to the Online State; if not, the module transitions to the Offline State.

State 7: Online State

The module is connected with a GPC through the USB port. In this state, the USB icon is displayed at the upper left corner of the LCD port. The module is driven by the JAVA applet through the communication protocol. The JAVA applet will send the different authentication requests to the module. The user needs to swipe his finger on the fingerprint sensor, and if the fingerprint matches the stored template, the module will get the relevant account number. If the fingerprint doesn't match, the module will display the "No Match" message on the LCD port and ask the user to swipe again. The module supports up to a maximum of 10 wrong swipes and then the module will be blocked. If the user doesn't swipe the finger for a 2 minute period the module will exit the swipe finger mode and wait for another command.

Once the user is authenticated, the module will get the relevant account number according to the authentication result. If the JAVA applet requires admin permission and if the account number corresponds to the Admin role, the module works as admin module. If the JAVA applet requires user permission and if it corresponds to the user role, the module works as user module, the module will ask user to authenticate again.

If any conditional test fails the module transitions to the Error State.

GPC can also send a command to the module to transition to the Power-off State.

State 8: Offline State

The module is not connected through the USB port. In this state, the USB icon is not displayed on the LCD. The module asks the user to swipe his/her finger for authentication.

The CM maintains a list of registered account numbers together with their corresponding fingerprints for authentication. If the module has multiple accounts registered, after authentication by a matching fingerprint, the user can select an already authenticated account. This means that the identification information does not need to be provided for the OTP service. It is rather specified via selection when such a need arises.

Once the module authenticates the user and the fingerprint corresponds to a user role, the module will display the dynamic PIN. Otherwise, the module will ask the user to authenticate again (notice that the Admin role cannot use the dynamic PIN service). After 40 seconds the module transitions to the Power-off State. If the module is connected with a GPC when the PIN is displayed then the module transitions to the Online State.

State 9: Power-off State

The module is completely switched off. The module doesn’t provide a manual switch off function but it can be switched off or reset by the JAVA applet. The power on switch can only be used to switch on the module. If the module runs out of battery, once the power button is pressed and it displays a “Low Battery” message through LCD port, then immediately switches off.

Physical Security

The primary means of the physical security for the module is the possession of the module. A customer security policy should be based on ensuring that only authorized personnel have access to the module at all times. This is implemented by the embedded fingerprint sensor. When a user tries to use the module, the first step is to swipe the registered fingerprint to authenticate itself.

The cryptographic module implements the tamper resistance functionality. The circuit board is covered by black color encapsulating resin during the manufacturing phase to avoid any access to the PCB. Additionally, the case is totally sealed by 2-component epoxy resin during the manufacturing phase. If the user attempts to open the module the case will be destroyed.

If the battery runs out of energy while the module is in storage, the real time clock will be cleared. Next time the module is switched on, the processor will erase all user information stored in flash memory.

The module will not function if the epoxy is broken. Exposing the components damages the device.

Operational Environment

The module uses flash memory to store all code and data. The flash memory is split into two parts; the read only area stores the MIIKOO Device Bootstrap, the MIIKOO Device Algorithm Library and the MIIKOO Device Application. The writeable area stores user information and CSPs.

GPC Operating System

The cryptographic module is classified as a "Multi-chip Standalone Cryptographic Module" for FIPS 140-2 purposes. It does not rely to any underlying Operating System or Supporting applications. It works together with a JAVA applet that runs on a connected GPC and a backend MIIKOO server in order to realize its functionality. The GPC could be running Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows Vista, Microsoft Windows 7, Linux and Mac OS X. An additional requirement for all above GPC operating systems is the installation of SUN JRE 1.6.0 or higher.

Object Model

Each cryptographic module is unique with its identification number and keys, and can only be accessed by one application at a time. In this regard other processes on the GPC have no access to that module and can therefore not interrupt or gain access to the information or activities contained within that module. In this way the cryptographic module protects the single user control of the cryptographic activities and data.

Rules of Operation for CM

1. Once the module is switched on it is initialized to the FIPS mode of operation.
2. The replacement or modification of the module or software by unauthorized intruders is prevented. The module may not be modified without destroying it.
3. The module itself enforces the authentication method by means of swiping a fingerprint to prevent unauthorized access to module services.
4. All critical security parameters are verified as correct and are securely generated, stored, and destroyed.

5. The unauthorized reading, writing, or modification of the communications interface of the module is prohibited.

6. The writable memory areas of the module (data and stack segments) are accessible only by a single JAVA applet so that the module is in "single user" mode, i.e. only one JAVA applet has access to that instance of the module.

7. Secret or private keys that are input to or output from the module must be input or output in encrypted form using a FIPS Approved algorithm.

8. There is no maintenance mode of the module. When the module encounters a problem, the owner needs to register a new one. The old one will be destroyed and all the CSPs will be erased.

9. The module should be recharged at least every 6 months. This could be done by plugging the module to GPC or wall adapter.

Rules of Operation for GPC

1. The referencing JAVA applet accessing the module runs in a separate virtual address space with a separate copy of the executable code.

2. All GPC operating system components that can contain sensitive cryptographic data (main memory, system bus, disk storage) must be located in a secure environment.

3. No unauthenticated operation is allowed to access CSPs. All of the services that can be called by the Java applet are listed in Table 6. The authentication column indicates the required authenticate for calling each service.

Cryptographic Key Management

Key Storage

The module provides long-term cryptographic key storage. It stores all the keys in a separate area of its embedded flash memory. This area can only be accessed by the JAVA applet using the encrypted communication protocol. All the other methods are prohibited and will cause the micro processor unit to erase the keys. File Key is stored in plaintext in the embedded flash memory, the Session key exists in plaintext only in RAM, and all other keys are stored encrypted in the embedded flash memory. Reference 17 describes the detailed key management.

Key Identifier	Key Type	Key Length
Handshake key	Triple-DES ECB mode	24 Bytes
File key	Triple-DES ECB mode	24 Bytes
Decrypt TSK key	Triple-DES ECB mode	24 Bytes
Session key	Triple-DES ECB mode	24 Bytes
TSK	Triple-DES ECB mode	24 Bytes
TMK	Triple-DES ECB mode	24 Bytes
TPK	Triple-DES ECB mode	24 Bytes
DSK	Triple-DES ECB mode	24 Bytes
PVK	Triple-DES ECB mode	24 Bytes
Certificate public key	RSA	1024 / 2048 bits
Certificate private key	RSA	1024 / 2048 bits
DSK	HMAC	24 Bytes

Table 14: Stored keys

Key Generation

Key generation is handled by using the FIPS 140-2 approved DRBG. It contains both true random number and pseudo random number generators.

The true random number generator uses oscillation loops which consist of inverters to generate random number seed, and then use this seed to produce true random number. Because of the true random characteristics of the seed, the generated random number also has true random characteristics. It can produce 1 to 128 bits width true random numbers, supports serial and parallel seed modes，supports interrupt，registers control to seed and generate random, support load 128bit parallel true random number seed.

The DRBG is implemented by FIPS-approved DRBG 800-90. It combines two different true random number generator results as a 32 byte input seed and produces a 32 byte number. DRBG re-seeds every time when DRBG function is called. The implementation of DRBG guarantees that the seed and the seed key will never be identical.

There are no intermediate key generation values output from the cryptographic module upon completion of the key generation process.

During key generation, no information is output from the cryptographic module until the operation is finished.

Key Establishment

The module performs a 2048 bits Diffie-Hellman symmetric key establishment to initialize the secure communication with the GPC. This method is based on NIST SP 800-56A.

Diffie-Hellman key agreement methodology provides 112 bits of encryption strength.

Key Protection

The management and allocation of the memory is the responsibility of the micro processor unit. It uses embedded flash memory area to store all the keys. The JAVA applet can only access the keys by using the encrypted communication protocol through USB port. Once the module is open or broke, the micro processor unit will be triggered to erase all the keys.

Key Zeroization

When the module is running, all keys and CSPs which are temporarily created in RAM will be zeroized with the memset() function when they are no longer used.

If the keys and CSPs stored in the flash are not used anymore (for example when deleting a registered account), the related keys and CSPs will be erased from the flash memory by filling zeroes into the corresponding address, so values are unrecoverable.

During key zeroization, no information is output from the cryptographic module until the operation is finished.

Key Import / Export

The module provides a series of services for JAVA applets to access cryptographic material stored inside. The module could also import public and private keys or export the

public keys in an encrypted format outside of the module through JAVA applet calls. The private key cannot be exported.

There is no manual key import and export method used in the module.

EMI / EMC

The FccID of the module is: Y6L-MIIKOO-004.

Reference 14 is Fcc certificate and reference 15 is Fcc test report.

Self Tests

The module automatically performs a number of power-on self-tests and conditional tests to ensure proper operation of the module. Power-on self-tests include cryptographic algorithm known answer tests and integrity tests. The integrity tests are performed using a SHA-256 digest calculated over the object code in the FIPS Object Module. Power-on self-tests will be automatically executed when the module is initialized. The JAVA applet can also control the module to run power-on self-tests by resetting the module. FIPS functionality won't be available until the successful execution of all power-up self-tests. No authentication is required to perform self-tests on power-up.

The failure of any self test causes the module to enter the Error State, and all cryptographic operations are disabled until the module is reset. Note that the most likely cause of a self test failure is memory or hardware errors. In practice, a self test failure means the module can't be used.

If the power-on self-tests are passed, the module will show a small "F" through LCD display port to indicate the FIPS_Mode.

Power-on Self-tests

Known Answer Test

Known Answer Tests (KATs) are tests where a cryptographic value is calculated and compared with a stored previously determined answer. The power-on self-tests for the following algorithms use KAT:

Algorithm	Known Answer Test
Triple-DES ECB and CBC mode	Encryption and decryption
HMAC	HMAC-SHA-256
RSA	Encryption and decryption by with 2048 bits key pair
SHA	SHA-256
CRC32	Checksum comparison
DRBG 800-90	Pseudo RNG generation

Table 15: Power-on self-tests

DRBG test

The first block (32 bytes) generated after power up or reset is not used and it is saved for comparison. Each subsequent 32 byte block is compared with the previously generated block,

as part of the conditional tests, which is performed every time before DRBG function is called. If the test fails, the module will display a FIPS error and switch off immediately.

Integrity test

The module implements the integrity test for both the firmware and algorithm library using SHA-256.

Only the Admin role can perform FIPS validated firmware update operation on the factory version module. The factory version module is the version of the firmware that has updating functionality, so that an Admin role can upload the FIPS 140-2 validated version of firmware into the CM through an initialization process to completely replace it. When the module is updated to FIPS validated firmware, the update function will be disabled. At the server side, it generates the SHA-256 value of the firmware, and then the firmware is encrypted by a temporary key using triple-DES. Server sends the SHA-256 value and the temporary key encrypted by TSK. During the firmware update, the server splits the encrypted firmware into several packages and adds the calculated CRC32 value to the end of each package. When the module receives the package, the first thing is to calculate the CRC32 value of each package and compare with the server calculated value. Once the module gets all packages it packs them into one file and calculates the SHA-256 integrity value of this file. This value is then compared with the one sent by the server: if they match, the micro processor unit will update the firmware, store the SHA-256 integrity value and zeroize the temporary key; otherwise the micro processor unit keeps using the current firmware, and the new firmware is discarded.

After successfully updating the FIPS validated firmware, every time the module is switched on, it will calculate the SHA-256 value of the firmware and compares it with the stored value. If both values match, the module will start the self test process. Otherwise, the module will display an error message and switch off after 3 seconds.

Conditional Tests

In addition to the power-on self-tests, the module performs several conditional tests including pair-wise consistency tests on newly generated public and private key pairs and continuous test for DRBG 800-90. If any of the conditional tests fails, the module will display a FIPS error and switches off immediately.

A pair-wise consistency test is performed when RSA key pairs are generated by applying a private key to decrypt the cipher text encrypted by the public key as well as applying a public key to decrypt the cipher text encrypted by the private key, and then verifying that the result equals the original plaintext in both cases.

A DRBG800-90 test is performed when the module generates random numbers. The first generated random number will be used only as reference. Then the module will generate a second random number and compare it with the previous one, if they do not match then the second one will be returned as the generated random number and used as the new reference. If both random number values are the same then the module will display “FIPS ERR” and switches off automatically after 3 seconds.

Algorithm	Conditional Test
RSA	Pair-wise consistency test (public encryption and private decryption with 2048 bit key)
DRBG 800-90	Continuous DRBG test

Table 16: Conditional tests

Design Assurance

The module is managed in accordance with the established configuration management and source version control procedures, with additional mechanisms to assure the integrity of source code as delivered and used to create applications.

Source Code Control

The development of the module software and hardware (configuration management, version control, change control, software defect tracking) are managed by the Pierson Capital Technology LLC. All document revisions are maintained in a TortoiseSVN 1.6 repository (http://svn.mobi-k.com:8000/svn/) with read and write access restricted to the core MIIKOO development team.

Address	Read/Write	Member
http://svn.mobi-k.com:8000/svn/public	R/W	All teams
http://svn.mobi-k.com:8000/svn/hardware	R/W	Hardware team
http://svn.mobi-k.com:8000/svn/firmware	R/W	Firmware team

Table 17: Source code control repositories

Mitigation of Other Attacks

The module does not contain any specific mitigation of other attacks.

Glossary

AES	Advance Encryption Standard
API	Application Programming Interface
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
DSK	Device Secret Key
ECB	Electronic Codebook
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FAR	False Acceptance Rate
FIPS	Federal Information Processing Standard
FPGA	Field-Programmable Gate Array
FRR	False Rejection Rate
FSM	Finite State Machine
GPC	General Purpose Computer
GPIO	General Purpose Input / Output
HMAC	Hash based Message Authentication Code
IIC	Inter-Integrated Circuit
JTAG	Joint Test Action Group

LCD	Liquid Crystal Display
LDO	Low Dropout regulator
MPU	Micro Processor Unit
NIST	National Institute of Standards and Technology
OS	Operating System
OSC	Oscillator
OTP	One Time Password
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PVK	PIN Verification Key
RSA	Rivest, Shamir and Adleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SPI	Serial Peripheral Interface
Triple-DES	Triple Data Encryption Standard
TMK	Terminal Master Key
TPK	Terminal PIN Key
TSK	Transport Key
UART	Universal Asynchronous Receiver/Transmitter
USB	Universal Serial Bus

References

1. FIPS PUB 140-2, Security Requirements for Cryptographic Modules, 12-03-2002, National Institute of Standards and Technology
2. Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, 24 March 2004 (draft), National Institute of Standards and Technology
3. Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, 13 April 2010, National Institute of Standards and Technology
4. NIST Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, 19 May 2008, National Institute of Standards and Technology
5. NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation Methods and Techniques, Dec 2001, National Institute of Standards and Technology
6. FIPS PUB 180-3, Secure Hash Standard (SHS), Oct 2008, National Institute of Standards and Technology
7. NIST Special Publication 800-57, Recommendation for Key Management – Part 1: General (Revised), Mar 2007, National Institute of Standards and Technology
8. MIIKOO Device Applet Handshake, Jun 2011, Pierson Capital Technology, LLC
9. MIIKOO Device Applet Protocol, May 2011, Pierson Capital Technology, LLC
10. MIIKOO Device Manual, Jun 2010, Pierson Capital Technology, LLC
11. MIIKOO Device D4 Specification, Nov 2010, Pierson Capital Technology, LLC
12. Performance Test Report of Synochip Algorithm (AS508) v1.5, Sep 2011, Hangzhou Synochip Technologies Co., Ltd.
13. MIIKOO System Initialization, Mar 2011, Pierson Capital Technology, LLC
14. GRANT OF EQUIPMENT AUTHORIZATION, 19 Jan 2011, Nemko Canada Inc.
15. Fcc Report, 19 Jan 2011, Shenzhen EBO Technology Co., Ltd.
16. MIIKOO Account Registration, Jun 2011, Pierson Capital Technology, LLC

17. MIIKOO Key Management, May 2011, Pierson Capital Technology, LLC

18. MIIKOO Module Services, May 2011, Pierson Capital Technology, LLC