UniMate USB/TRRS PKI Token FIPS 140-2 Security Policy

Document Version: 1.3

Date: 2015-01-04

Prepared for:

SecuTech Solutions PTY LTD

Suite 514, 32 Delhi Road,

North Ryde, NSW 2113

Australia

Prepared by:

atsec information security corporation

www.atsec.com

9130 Jollyville Road, Suite 260

Austin, TX 78759

United States of America

Table of Contents

Tables

Figures

1. Introduction

This document is a non-proprietary FIPS 140-2 Security Policy for the UniMate USB/TRRS PKI Token cryptographic module (hereafter also referred to as “UniMate token,” “UniMate,” “token,” or “module”) manufactured by SecuTech Solutions PTY LTD. It describes how the token meets the requirements as specified in FIPS PUB 140-2 (Federal Information Processing Standards Publication 140-2) for a Security Level 2 multi-chip standalone hardware module.

The Security Policy is required for FIPS 140-2 validation and is intended to be part of the package that is submitted to the Crypto Module Validation Program (CMVP). It describes the capabilities, protection, and access rights provided by the cryptographic module. It also contains a specification of the rules under which the token configure to operate in FIPS mode. This security policy allows individuals and organizations to determine whether the cryptographic token meets their security requirements and to determine whether the module, as implemented, satisfies the stated security policy.

The targeted audience of this document consists of, but not limited to, the SecuTech and its application developers, testers at the Cryptographic Services Testing (CST) lab, and reviewers from CMVP.

This security policy is one document used for a FIPS 140-2 validation. In addition to this document, the following documents also serve as the supporting evidence for the FIPS 140-2 validation:

- UniMate USB/TRRS PKI Token Quick Guide (Version 2.0)
- UniMate USB/TRRS PKI Token Card Operating System Manual (Version 3.1)
- UniMate USB/TRRS PKI Token Finite State Machine (Version 1.1)

With the exception of the Non-Proprietary Security Policy, the FIPS 140-2 validation documentation is proprietary to SecuTech. For access to these documents, as well as answers to other technical or sales-related questions for the module, please contact SecuTech. The SecuTech contact information is posted on the NIST CMVP website (http://csrc.nist.gov/groups/STM/cmvp/validation.html).

2. Cryptographic Module Specification

2.1. Module Overview

The UniMate USB/TRRS PKI Token is designed for PKI applications using digital signature and strong authentication. After the token is properly initialized, it is a PKI-based authenticator which contains necessary firmware and hardware to balance security with easy-to-use features. It is a combination of cryptography, smartcard, and other advanced technologies. The UniMate token is used as the container of keys and certificates for the two-factor authentication as well as the crypto processor. It provides digital signature generation/verification services for online authentications and data encryption/decryption services for online transactions. It provides the convenience of allowing the user to visually confirm the transaction through the UniMate's LCD display screen before he or she proceeds with the signing operation. The user's RSA private and public key pairs can be either generated by the UniMate token or imported into the token and then stored in its embedded Smart Card chip. If the RSA key pair is generated by the UniMate token, its private key can never be exported.

The UniMate token provides a USB port and a 3.5mm TRRS audio jack port connector. It can connect to a General Purpose Computer (GPC) via USB port or a mobile device such as iPhone, iPad, iTouch, Android phones and tablets via audio port in a "plug and play" manner. It is ideal for online banking where transactions can be visually inspected before the digital signing. Regardless whether the online banking is conducted on a GPC or a mobile device, the UniMate token provides the desired protection for both.

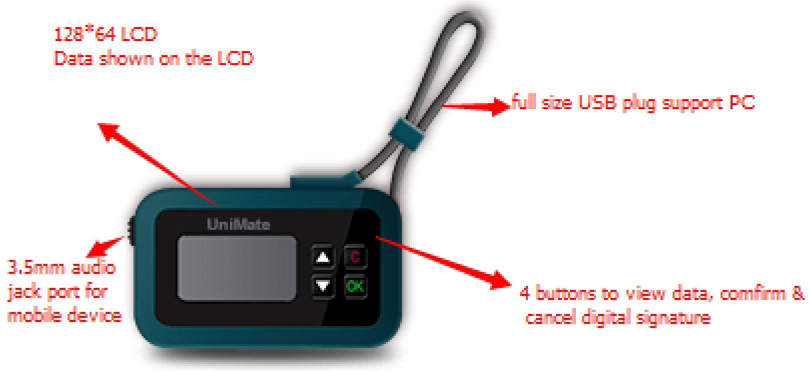
128*64 LCD
Data shown on the LCD
full size USB plug support PC
UniMate
C
OK
3.5mm audio jack port for mobile device
4 buttons to view data, comfirm & cancel digital signature

Figure 1: Front View of UniMate USB/TRRS PKI Token

The transaction data to be digitally signed is displayed on the built-in LCD screen. The user of the token can conveniently observe and confirm the transaction data before he decides either to push the green OK button to sign the transaction or to push the red C (for cancel) button to cancel the transaction. The white Up arrow and Down arrow buttons are for scrolling the display content on the LCD screen.

The UniMate implements type A USB 1.1 (full speed) specification and USB CCID (Circuit(s) Cards Interface Device) protocol which enables communication with ISO/IEC 7816 smart cards over USB. When the communication is established via TRRS audio jack port, analog signal will be transferred to digital by the A/D circuit and then the decoding module will transfer the digital signal to final signal that conform to CCID protocol. If both the USB port and the audio port are connected, then the USB port takes the precedence and the audio port will be blocked.

2.2. Cryptographic Module Description

The physical boundary of the UniMate USB/TRRS PKI Token is defined as the opaque enclosure surrounding the token device as shown in the picture below:

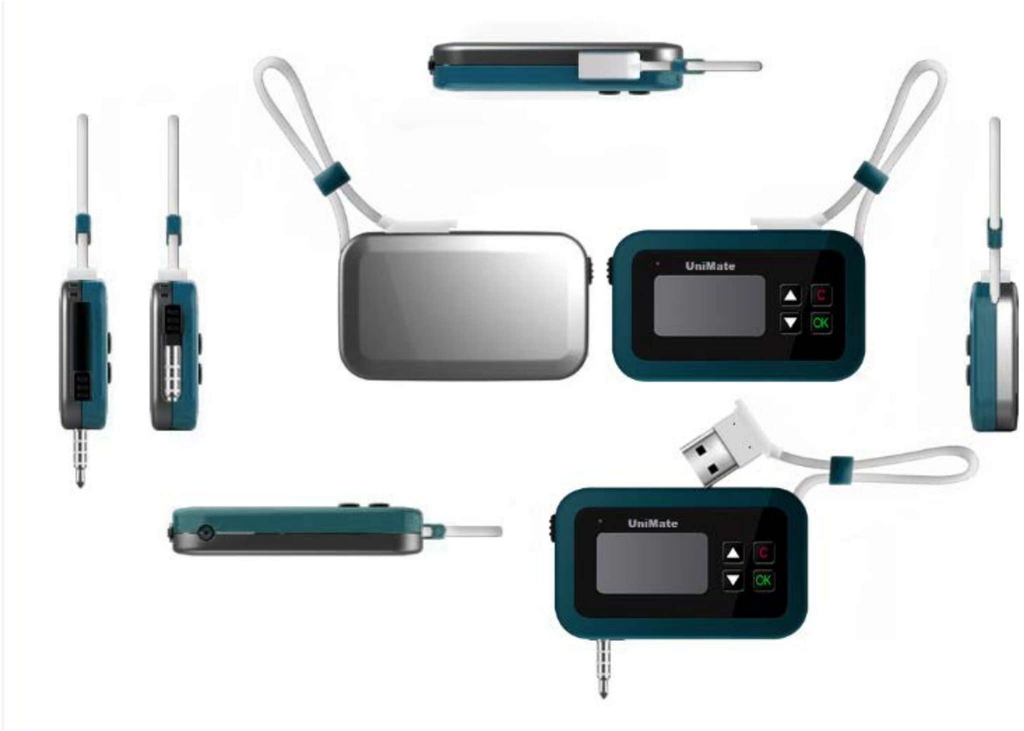

Figure 2: Multi-view of UniMate USB/TRRS PKI Token

The following table listed the hardware and firmware components of the cryptographic module:

Component Type	**Specification**
Hardware	Version: 2.11
	Model: Flex
	ID: globally unique 64 bits
	Dimensions: 65*36*11.4(mm)
	Weight: 23g
	Audio Jack Port: 3.5mm TRRS
	USB Port: Type A
	Smart Card IC chip: MCU-HS08K (Hongsi 08K)
	RAM: 4K
	On-chip Flash memory: 256K
	Off-chip Flash memory shown as Virtual CD-ROM:2M
	Power Supply: Lithium-Ion Rechargeable Battery
	Key Pad: Four Control Buttons(page up, page down, confirmation and cancellation)
	LCD Display:128 x 64 Points Monocolor Display
Firmware	UniMate USB/TRRS PKI Token, Version 5.1.6 (File name is UniMateFIPSFirmware2014-5-1-6.fw)

Table 1: UniMate USB/TRRS PKI Token Cryptographic Module Components

Once the firmware is loaded into the token, no other version of the firmware can be loaded into the token to replace the FIPS 140-2 validated version of the firmware.

2.3. Block Diagram

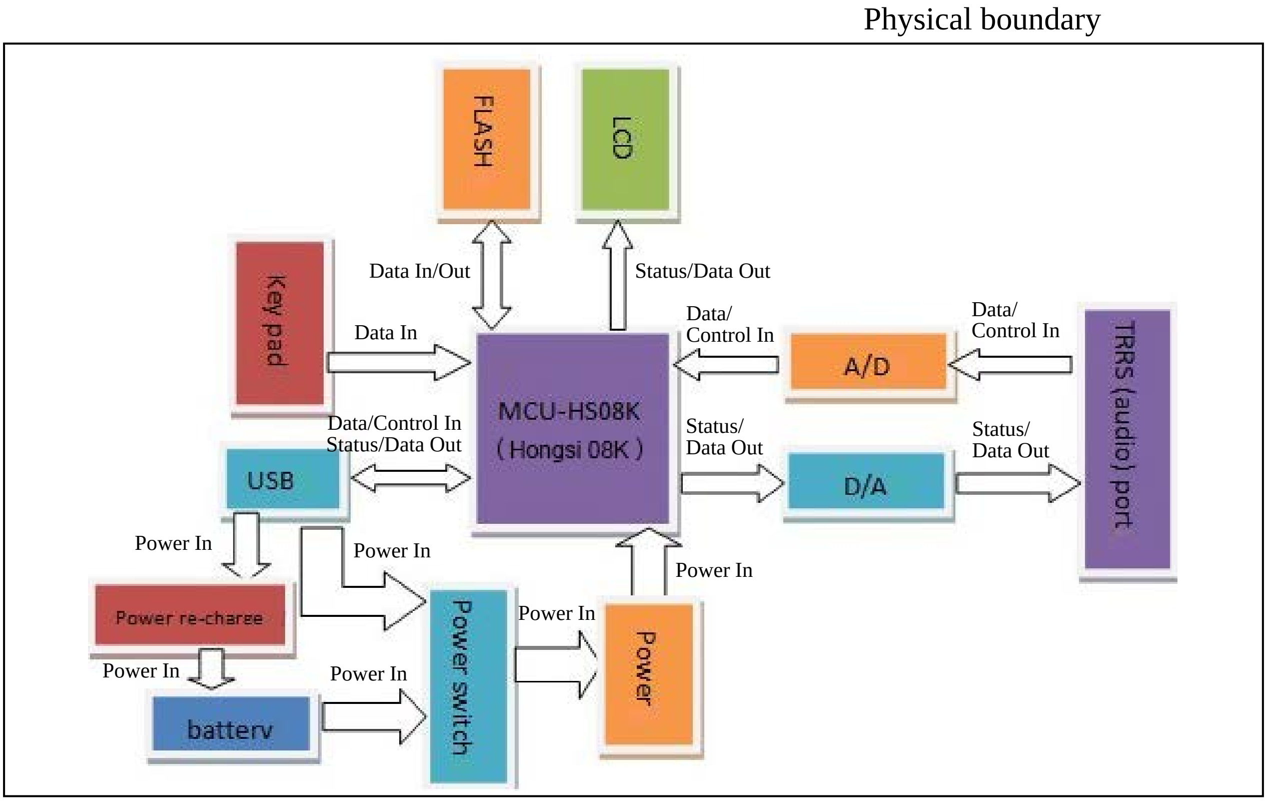

Figure 3: UniMate USB/TRRS PKI Token Hardware Block Diagram

2.4. Cryptographic Module Security Level

The module is validated as a multi-chip standalone hardware module against FIPS 140-2 at the overall Security Level 2. The following table shows the security level claimed for each of the eleven sections that comprise the FIPS 140-2:

FIPS 140-2 Sections	Security Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Cryptographic Module Ports and Interfaces	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	2

FIPS 140-2 Sections	Security Level
Mitigation of Other Attacks	N/A

Table 2: Security Levels for Eleven Sections of the FIPS 140-2 Requirements

2.5. Mode of Operation

The UniMate token has only FIPS-Approved mode of operation. The token provides all of the services in the FIPS mode. The following FIPS-Approved or FIPS-Allowed algorithms are implemented in the token:

Algorithm	Mode/CSPs	Usage	Standard	CAVP Certificate #
AES	Mode: ECB, CBC 128, 192, 256 bit keys	Encryption/ Decryption	FIPS 197	2836
Triple-DES	Mode: ECB,CBC 3-key 168 bits	Encryption/ Decryption	SP 800-67	1696
SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	N/A	Hashing	FIPS 180-4	2377
RSA Key Generation	Module sizes: 2048, Public Key size: 65537	Generate 2048 bits RSA Key pairs	FIPS 186-4	1478
RSA Signature Generation based on PKCS#1 v1.5	Module size: 2048, Public Key size: 65537, SHA-224/256/384/512	Generate RSA signature	FIPS 186-4	1478
RSA Signature Verification based on PKCS#1 v1.5	Module size: 2048, Public Key size: 65537, SHA-224/256/384/512	Verify RSA signature	FIPS 186-4	1478
DRBG	CTR DRBG, AES-128 bit, Derivation function, Support prediction resistance	Generate random number	SP 800-90A	492
HMAC-SHA	At least 112 bits	Firmware	FIPS 198-1	1777

Algorithm	Mode/CSPs	Usage	Standard	CAVP Certificate #
-1	HMAC key	integrity check		
CMAC	3-key Triple-DES MAC	Generate/ Verify Message authentication code	SP 800-38B	1696
HW RNG	Entropy source input 128 bits Random output per access	The HW RNG output is used to seed the FIPS Approved DRBG	N/A	No CAVS test available

Table 3: FIPS-Approved or FIPS-Allowed Cryptographic Algorithms

3. Cryptographic Module Ports and Interface

The physical ports of the UniMate token and their usages are the following:

- USB port and audio jack port are the data in and data out interfaces
- Four control buttons on the Key Pad consists of the control in interface
- LCD screen is the status out interface

The logical interface of the UniMate token consists of a set of Application Protocol Data Unit (APDU) commend-response pairs. A command APDU is sent to the UniMate token that contains a mandatory 4-byte header (CLA, INS, P1, P2) and from 0 to 255 bytes of data. A response APDU is sent by the UniMate token that contains a mandatory 2-byte status word and from 0 to 256 bytes of data. The structure of an APDU command-response pair is shown in the table below:

Command APDU		
Field Name	Length (bytes)	Description
CLA	1	Instruction class indicating the type of command, e.g., inter-industry or proprietary
INS	1	Instruction code indicating the specific command, e.g., “select file”
P1-P2	2	Instruction parameters for the command, e.g., which file to select
Lc	0, 1 or 3	Number of bytes of command data to follow
Command data	Nc	Lc bytes of data
Le	0, 1, 2 or 3	Maximum number of response bytes expected
Response APDU		
Response data	Nr	Response data with length r be less than or equal to Le
SW1-SW2 (response trailer)	2	Command processing status, e.g., 9000 (hexadecimal) for success

Table 4: Structure of an APDU Command-response Pair

The module will process only one command APDU at a time and must process the corresponding response APDU before allowing another APDU command to be processed. The module does not support concurrent operators.

The module implements a subset of command APDUs defined in the ISO/IEC 7816-4. In addition, the module also implements some customized APDUs.

The following table shows the mappings between the required logical interface by the FIPS 140-2 standard and the physical ports as well as the logical interface of the module in terms of the fields of the APDU Command-Response pair:

FIPS 140-2 Required Logical Interface	UniMate Physical Ports Using USB Connection	UniMate Physical Ports Using Audio TRRS Connection	Fields of APDU Command-Response Pair
Data Input	Data pins within the USB Port ()	Left audio channel within the TRRS Port	Lc, Command Data Field
Data Output	Data pins within the USB Port	Left audio channel within the TRRS Port	Response Data Field
Control Input	Four control buttons on Key Pad	Four control buttons on Key Pad	CLA, INS, P1, P2, Le
	Data pins within the USB Port	Left audio channel within the TRRS Port	
Status Output	Data pins within the USB Port	Left audio channel within the TRRS Port	SW1, SW2
	LCD display	LCD display	
Power Input	Power pin within the USB Port	Internal battery	-

Table 5: Port and Interface of UniMate token

4. Roles, Services, and Authentication

4.1. Roles

UniMate USB/TRRS PKI Token supports three types of roles: Issuer, Admin, and User. The Issuer role and Admin role are considered for the purpose of FIPS 140-2 validation as the Crypto Officer role.

The Issuer role is authenticated by verifying a 168-bit Triple-DES key known as the Issue Key. Admin and User roles are authenticated by verifying an Admin PIN and User PIN, respectively. An Admin PIN or User PIN must be 8 to 24 characters long. There is only one Issue Key and one Admin/User PIN per token.

The UniMate token has an embedded smart card chip, which has an on-Card Operating System (COS) and on-Card File System (CFS). The smart card chip provides the overall desired security features for the UniMate token. To understand the interaction between the role authentication and the security mechanisms built into the UniMate token, it is necessary to understand the structure and access control of the CFS.

The CFS of the module complies with ISO/IEC 7816-4 and supports multiple levels of directory structure. An example of four-layer CFS is shown in the following figure:

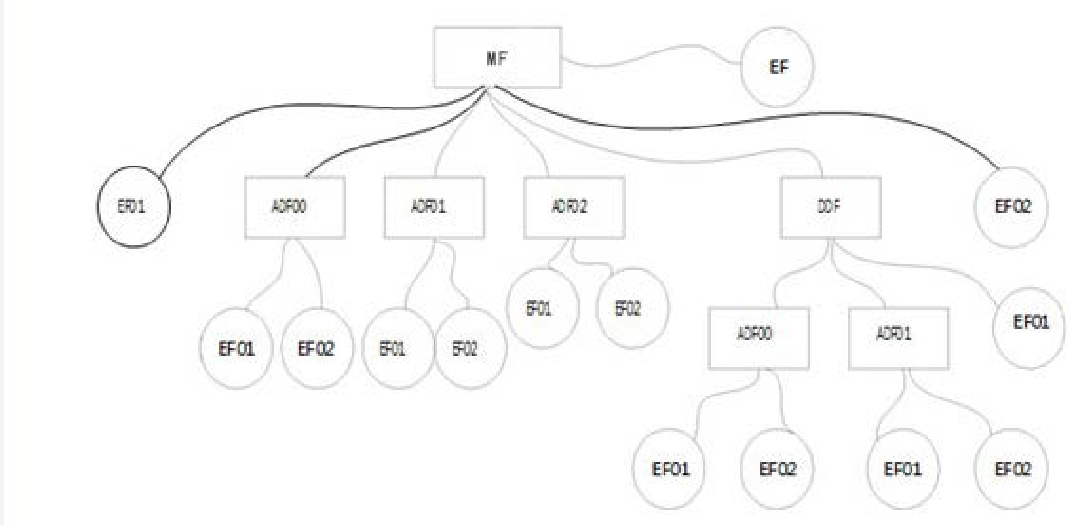

Figure 4: Example of Four-Layer on-Card File System

In the above figure:

- MF (Master File): It is the root directory of the entire file system. This folder exists when the token is manufactured by SecuTech.

- DDF (Directory Definition File): It is used to create an application environment, in which child directory files (ADF), elementary files (EF) and Authentication Key Files (i.e., a special kind of EF) can be created and stored. In DDF, only ADF or EF can be created and stored. No DDF can be created under a DDF. The creation/modification/deletion of this file requires the Issuer authentication.

- ADF (Application Definition File): It is a directory file and intended to be used for one specific application. An ADF shall have its own independent Authentication Key File that provides the security measure just for this Application folder. In ADF, only elementary files (EF) can be created and stored. No ADF or DDF can be created under an ADF. The creation, modification and deletion of this file require the Issuer authentication.

- EF (Elementary File): It is a continuous storage of data. User PIN authentication is required to create/read/modify/delete the EF with the exception of the following three special kinds of key files:

- One special kind of EF is the Authentication Key File which has the file ID 00 00. The Authentication Key File is used to store the authentication keys including the Master Key, Maintenance Key, PIN Unblock Key, PIN Reload Key, External Authentication Key, Internal Authentication Key, PIN Reload Key, Admin PIN, and User PIN. Creating and updating the Authentication Key File requires Admin PIN authentication and the Master Key in User State. The various states of a token's lifecycle are explained in section 4.2. No key in the Authentication Key File can be read or deleted. If an Authentication Key File does not exist under a directory, then all files within this directory *cannot* be created read, modified or deleted.

- Symmetric Key File is another special kind of EF which has a file ID in the form of 0E XX, where XX ranges from 00 to 79. Symmetric Key File is a binary file used to store symmetric keys for data encryption. Importing and writing into a Symmetric Key File requires User PIN authentication. Keys in the Symmetric Key File can neither be read nor be exported.

- RSA Key File is the third kind of special EF that is used to store RSA key pairs for digital signature operations. RSA public keys are stored in RSA Key Files with file IDs in the form of 1E YY, where YY ranges from 00 to 7F, while the corresponding RSA private keys are stored in RSA Key Files with file IDs in the form of 1E ZZ, where ZZ ranges from 80 to FF. Importing and exporting an RSA public key requires User PIN authentication. Generating RSA key pairs also requires the User PIN authentication. An RSA private key can never be exported.

It is highly recommended that the Issuer creates all the necessary directories and files when the token is initialized. After creating a new directory file (e.g., DDF or ADF), an Authentication Key File under this directory shall be first and foremost created. Then Admin PIN, User PIN and External Authentication Key (if applicable) should be added to the Authentication Key File. The designed security mechanism will become effective only after the necessary PINs and keys have been added in the Authentication Key File. Each directory of the on-Card File System can have a pair of Admin/User PINs that controls the access to the files in this directory upon the required authentication. The module does not support bypass capability.

Each file, upon its creation, has its associated security attributes defined in the file header. The security attributes of a file specify which operations (e.g., read, write, add, delete, etc.) can be applied to this file under what kind of authentication (e.g., Master Key, Maintenance Key, External Authentication Key, Internal Authentication Key, Admin PIN, User PIN, PIN Unblock Key, PIN Reload Key).The COS of the UniMate token enforces the security according to the security attributes of the files in the CFS. Therefore, it is crucial that upon the creation of a file, the desired security is set properly via its security attributes. For the details of how to create a file on the CFS of the UniMate token, the reader is referred to *UniMate USB/TRRS PKI Token Card Operating System Manual*.

The Issuer Role can update the Issue Key and initialize the token by creating directories, files and importing keys.

The Admin Role is for managing the token device and User Role. The Admin can lock the token device, import/change Authentication Keys, unblock the User PIN, reload the User PIN, write/erase data to/on the external SPI Flash, add/remove virtual CD-ROM, and reset counter.

The User Role can execute all of the approved algorithms, create general EF files, read/update/delete general EF files requiring User PIN, change the User PIN, and generate/update/import encryption keys stored in symmetric/asymmetric Key Files.

The details of the available services for each role are given in the following section.

4.2. Services

The UniMate USB/TRRS PKI Token provides all of its services through APDU commands and response messages. During the life cycle of the UniMate Token, it goes through the Manufacture State, Pre-personalization State and User State as explained below:

- Manufacture State: The UniMate Token is in this state when it is in the manufacture process. In this state, no security mechanism is applied and only the Issuer is allowed.

- Pre-personalization State: The UniMate Token is set to the Pre-personalization State at the end of the manufacture process. In this state, the on-Card File System can be initialized. No security mechanism is applied and only the Issuer is allowed in this state. In general, SecuTech follows the manufacture process with a pre-personalization process to initialize the token by setting up the necessary file system for their customers.

- User State: The UniMate Token is set to the User State at the end of the Pre-personalization. When the UniMate Token is shipped to SecuTech’s customers (either an issuer like a bank or an end-user), the token is in the User State. In this state, a user can use the services provided by the module for his PKI applications. The Issuer can use the Issue Key to call FORMAT DEVICE to rollback the UniMate Token from User State to Manufacture State.

The UniMate Token can only be degraded from the Manufacture State to Pre-personalization State and then to the User State. When the Issuer Role re-initializes the file system, the token can be reset to the Manufacture State from the User State.

Some services are only available in the Manufacture State. Some are available in both Manufacture State and Pre-personalization State, but not in the User State.

The following two tables list all of the services provided by the module. The first table contains all of the services that do not need authentication. There may be some keys or Critical Security Parameters (CSPs) used by these non-Authenticated services, but these services do not create, modify, disclose, or substitute keys and CSPs. The non-Authenticated services are available to all roles. The services listed in the second table require role-based authentication. For each service, a brief service description, the CLA and INS fields of the APDU message and the usage of CSPs (if applicable) are provided. For the other fields of the referenced APDU messages, the reader is referred to *UniMate USB/TRRS PKI Token Card Operating System Manual*. If a service is only available in a certain state or states of the token’s life cycle, it is indicated so.

4.2.1. Non-Authenticated Services

Service	Descriptions	CSP(s) Used
GET WORKING MODE	Returns the information of the working state of the UniMate Token such as enable/disable audio port communication, button, LCD display, LED functions. CLA: 00 INS: A3	None
CHANGE LANGUAGE	Changes the LCD display language between English and Chinese. CLA: 00 INS: A2	None
GET LANGUAGE	Returns the currently LCD display language. CLA: 00 INS: A6	None
CHANGE SIGNATURE SHOW	Enables or disables showing the transaction data on LCD for the RSA signing operation.	None

Service	Descriptions	CSP(s) Used
	CLA: 00 INS: A5	
GET SIGNATURE STATE	Returns the current state of whether the transaction data subject to RSA signing operation is shown on the LCD. CLA: 00 INS: A7	None
ENUMERATE FILE	Gets file IDs of all files of the specified type except key file in the current directory. CLA: 80 INS: 3A	None
EXTERNAL AUTHENTICATE	Authenticates an external entity to the UniMate Token. This service may also be used to both authenticate and initiate a secure session with an external entity. A maximal number of attempts can be set when the external authentication key is created. If the authentication fails, the remaining number of attempts for the referenced key decreases by one. If the authentication succeeds, this number will be reset to the maximum. CLA: 00 INS: 82	External Authentication Key
GET EXTERNAL INFO	Returns the maximum attempts and the current remaining attempts of the external authentication for the currently selected application directory. CLA: 80 INS: DB	None
GET DEVICE INFO	Gets device information of the UniMate Token such as its factory information, issuer information and hardware version. CLA: 80 INS: 38	None
GET CHALLENGE	Requests a random number that will be used as a challenge within the External Authentication service. CLA: 00 INS: 84	DRBG Seed, Random Number

Service	Descriptions	CSP(s) Used
GET PIN INFO	Gets the maximum number of attempts and the current remaining number of attempts of the selected PIN in the key file of the current directory. This service also provides confirmation whether the current PIN is identical to its factory default value. CLA: 80 INS: 50	None
GET RESPONSE	Gets response data immediately after a command APDU message. CLA: 00 INS: C0	None
GET VERSION	Gets firmware information of the UniMate Token, which is 5.1.6, and the firmware building date. CLA:00 INS: A1	None
GET VIRTUAL CD-ROM STATUS	Returns the virtual CD-ROM status. CLA: 00 INS: B6	None
INTERNAL AUTHENTICATE	Authenticates the UniMate Token to an external entity. CLA: 00 INS: 88	Internal Authentication Key
LOG OFF	Logs off the currently authenticated Admin Role or User Role by removing the admin or user logon state information. CLA: 00 INS: D9	None
RESET RAM	Clears RAM CLA: 00 INS: F6	None
SELECT FILE	Selects the file of the given file ID. CLA: 00 INS: A4	None
SELECT RSA KEY	Selects the RSA key pair with the given key ID as the current RSA key pair. When the key ID is not provided, this APDU command will clear the selection for the current RSA key pair.	None

Service	Descriptions	CSP(s) Used
	CLA: 80 INS: 42	
SELF TEST	Performs FIPS 140-2 required self-tests on-demand. CLA: 00 INS: F3	None
SOFT RESET	Zerorizes the RAM, and all the data, registers or counter in RAM will be cleared. CLA: 00 INS: F1	None
VERIFY PIN	Verifies Admin PIN or User PIN provided in the data field of the APDU command against the corresponding PIN saved in the key file of the current selected directory. Only one role can be authenticated at a time. CLA: 00 INS: 20	Admin PIN or User PIN

Table 6: Non-Authenticated Services

4.2.2. Authenticated Services

Services	Descriptions, Input and Output	Authenticated Role	Keys or CSPs
ADD/REMOVE VIRTUAL CD-ROM	Enables/disables virtual CD-ROM, which is used to store software for token customers to run on the host PC or mobile device. CLA: 00 INS: B5	Admin	Admin PIN
APPEND RECORD	Appends a record to fixed-length record or variable-length record to an EF. CLA: 00 or 04 or 80 or 84 INS: E2	User	User PIN
APPLICATION BLOCK	Disables the current application (ADF), then all the files under this ADF are not	User	User PIN and Master Key

Services	Descriptions, Input and Output	Authenticated Role	Keys or CSPs
	accessible. CLA: 84 INS:1E		The index of the Block Key is stored in the Authentication Key File.
APPLICATION UNBLOCK	Enables the current application. (ADF) CLA: 84 INS: 18	User	User PIN and Master Key The index of the Block Key is stored in Authentication Key File.
CHANGE ISSUE KEY	Changes Issue Key. CLA: 00 INS: D8	Issuer	Issue Key Note: Only available in the Manufacture State.
CHANGE LIFECYCLE STATE	Changes the lifecycle state of the UniMate Token from Manufacture State to Pre-personalization State, and from Pre-personalization State to User State. CLA: 00 INS: EE	Issuer	None Note: Only available in the Manufacture or Pre-personalization State.
CHANGE PIN	Changes Admin or User PIN, or resets User PIN. CLA: 00 INS: 5E	User or Admin	User PIN or Admin PIN If the User PIN is reseted, the Admin PIN and the PIN Reload Key are needed.
CHANGE WORKING MODE	Changes the working state of the UniMate Token such as enable/disable audio port communication, button, LCD display, LED functions. This	Issuer	None Note: Only available in the Manufacture

Services	Descriptions, Input and Output	Authenticated Role	Keys or CSPs
	service is only available in the Manufacture State. CLA: 00 INS: F4		State.
CREATE FILE	Creates a file or a directory on the card file system. CLA: 00 or 04 INS: E3	Issuer, User	In Manufacture or Pre-personalization State: no security mechanism In User State: User PIN and Master Key The index of the Block Key is stored in the Authentication Key File. The permission inherits from initialization or upper directory. Note: directories can only be created by the Issuer in the Manufacture State or Pre-personalization State.
DELETE FILE	Deletes a file from the card file system. CLA: 00 or 04 INS: 0E	User	User PIN and Master Key The index of the Block Key is stored in Authentication

Services	Descriptions, Input and Output	Authenticated Role	Keys or CSPs
			Key File. The permission inherits from initialization or upper directory.
DEVICE BLOCK	Disables the token. If the device is blocked, all functions are disabled, except format device. CLA: 84 INS: 16	Admin	Admin PIN and Master Key The index of the Block Key is stored in MF.
ERASE SPI FLASH	Erases all the data stored in SPI Flash. CLA: 00 INS: B4	Issuer or Admin	In Manufacture or Pre-personalization State: : no security mechanism In User State: Admin PIN
FORMAT DEVICE	Formats the card file system, MF, and MF's key file are created. Other files or directories will be erased, so the token will in Manufacture State. CLA: 00 INS: D5	Issuer	In Manufacture or Pre-personalization State: no security mechanism In User State: Issue Key
GET BUTTON SW	Get key-pressing result CLA: 00 INS: C1	User	None
GENERATE RSA KEY	Generates a FIPS 186-4 compliant RSA 2048 key pair within the token. CLA: 80 INS: CE	User	User PIN, RSA key pair
GENERATE SYMMETRIC KEY	Generates a symmetric key using DRBG 800-90A algorithm implemented within	User	User PIN, AES key or Triple-DES key

Services	Descriptions, Input and Output	Authenticated Role	Keys or CSPs
	the token. CLA: 80 INS: CF		
HASH	Calculates the digital digest of data. CLA: 80 INS: CA	User	User PIN
PIN UNBLOCK	Unblocks the PIN. CLA: 84 INS: 24	Admin	Admin PIN and PIN Unblock Key
READ BINARY	Reads a binary file. CLA: 00 or 04 or 80 or 84 INS: B0	User	User PIN
RESET COUNTER	Resets the attempt counter to the maximum value. CLA: 00 INS: B8	Admin	Admin PIN
RSA SIGNATURE VERIFY	Verifies RSA digital signature with RSA public key. CLA: 80 INS: C4	User	User PIN, RSA key pair
RSA SIGNATURE GENERATION	Generates RSA digital signature with RSA private key. CLA: 80 INS: C2	User	User PIN, RSA key pair
READ RECORD	Reads a record file from an EF. CLA: 00 or 04 or 80 or 84 INS: B2	User	User PIN
READ SPI FLASH	Reads data from SPI Flash. CLA: 00 INS: B3	Issuer	None Note: Only available in the Manufacture State
SYMMETRIC OPERATE	Encrypts or decrypts data with a symmetric key. CLA: 80 INS: C8	User	User PIN, AES key or Triple-DES key
UPDATE BINARY	Updates binary file. CLA: 00 or 04 or 80 or 84	User	User PIN

Services	Descriptions, Input and Output	Authenticated Role	Keys or CSPs
	INS: D6		
UPDATE RECORD	Updates record file. CLA: 00 or 04 or 80 or 84 INS: DC	User	User PIN
WRITE KEY	Writes keys (except Issue Key) to Authentication Key File. CLA: 84 IND:D4	Issuer or Admin	In Manufacture or Pre-personalization State: no security mechanism In User State: Admin PIN and Master Key or Master Key in parent directory (if no Master Key in current directory) or Maintenance Key or Issue Key (no Master Key in parent directory)
WRITE SPI FLASH	Writes data to SPI Flash. The SPI Flash is used to store font and the virtual CD-ROM files. CLA: 00 INS: DE	Issuer or Admin	In Manufacture or Pre-personalization State: : no security mechanism In User State: Admin PIN

Table 7: Services Authorized for Roles

4.3. Operator Authentication

UniMate USB/TRRS PKI Token uses role-based authentication to authenticate different roles. The Issuer Role is authenticated by verifying a 168-bit Triple-DES key. The Admin Role and User Role are authenticated by verifying the PINs for the corresponding roles. In User State, the module can switch between Admin role and User role by calling the LOG OFF APDU command and re-authenticated with the

Admin PIN or User PIN. The Issuer role takes higher priority than the Admin role and User role when the operator assumes the Issuer role.

4.3.1. Authentication Strength

Because the Issue Key is 168-bit long, the probability of a successful random attempt to guess it is $1/2^{168}$, which is much less than 1/1,000,000. The UniMate Token takes 200ms to process one APDU that verifies an Issue Key. It can process at most 300 (i.e., 60 * 1000ms/200ms) Issue Key verification attempts within one minute. Therefore, the success rate of guessing the 168-bit Issue Key within a minute is $300/2^{168}$, which is much less than 1/100,000.

PINs for Admin and User are 8-24 characters long. The characters can be alpha-numerical and case sensitive, yielding at least 62 choices per character. The probability of a successful random attempt is at most $1/62^{8}$, which is less than 1/1,000,000.The UniMate Token locks the Admin account or User account after, at most, 15 consecutive failed authentication attempts; thus, the maximum number of attempts in one minute is 15. Therefore, the probability of a success with multiple consecutive attempts in a one-minute period is $15/62^{8}$, which is less than 1/100,000.

4.3.2. Authentication Data

The Issue Key is saved in the UniMate Token in plain text with the fixed length of 24-byte. Admin and User PINs are padded (if needed) to 24-byte fixed length and stored in the UniMate USB/TRRS PKI Token in plaintext.

The module ensures that there is no visible display of the authentication data, such as Issue Key, Admin PIN or User PIN. The authentication data is stored in the Authentication Key File(s) that can never be exported outside the token. All of the authentication states are stored in the RAM area. When the module’s power is off, all of the states will be cleared.

There are an initial Issue Key, initial Admin PIN and initial User PIN stored at the Authentication Key File under the root directory MF of the on-Card File System within UniMate USB/TRRS PKI Token when the token is manufactured. The initial Issue Key and PINs are distributed to SecuTech’s customers (e.g., a bank) in a secure manner compliant to SecuTech’s corporation security handling process and procedure. SecuTech strongly recommends their customers to change the initial Issue Key and PINs immediately after the tokens are received. The issuer of the UniMate Token may further create some directories on the on-Card File System as needed. For each directory, the issuer may create default Admin PIN and User PIN that governs the access to the files within this directory. When the end-user receives the UniMate Token issued by an issuer, he/she shall immediately change the default PINs.

5. Physical Security

The module is a multiple-chip standalone module and conforms to Level 2 requirements for physical security. The module is composed of production-grade components and is housed in a sealed, hard plastic enclosure that has no openings, vents, or doors. It cannot be opened without noticeable damage.

6. Operational Environment

The module operates in a limited non-modifiable operational environment and does not implement a General Purpose Operating System. The operational environment requirements do not apply to the module.

7. Key Management

7.1 Random Number Generator

The UniMate USB/TRRS PKI Token implements and uses a FIPS-Approved Deterministic Random Bit Generator (DRBG) based on SP 800-90A for random number generation and key generation. The UniMate implements a block cipher DRBG, CTR_DRBG, which generates a minimum of 128-bit of random value per request.

The token contains an IC hardware-based NDRNG (HW RNG) that provides 7.999 bits of entropy per byte. The HW RNG supplies 128 bits of seed to the DRBG 800-90A allowing generation of the random number to 128 bits of entropy.

7.2 Key Generation

The module uses the output of FIPS-Approved DRBG SP 800-90A as input to create the following keys/CSPs:

- AES/Triple-DES symmetric keys

- 2048 RSA key pairs

Each call of symmetric key or RSA key pair generation, the module calls HW RNG and reseeds the SP 800-90A for random number generation. In an addition, after each call of symmetric key or RSA key pair generation, the reseed counter is increased by 1. When the reseed counter value reaches a threshold, the module reseeds the SP 800-90A DRBG again and re-set the counter to 0. When generating a pair of RSA keys, the module uses the algorithm specified in DRBG SP 800-90A to generate a group of random numbers as the algorithm input parameters, and then uses these random numbers to generate the key pair in accordance with the RSA key generation algorithm described in FIPS 186-4.

7.3 Key Entry and Output

A User or an Admin enters his or her password manually using the keyboard of the host device to which the UniMate token is connected to. The SecuTech middleware running on the host device converts into a 24-byte binary string with appropriate padding if needed and sends it using the Verify & Change PIN APDU commands to the UniMate token for verifying or changing the PIN stored on the token. The middleware is outside the module boundary.

When the APDU command requires any keys, such as the Issue Key, Reload PIN key, symmetric keys, internal authentication key, external authentication key and master key to perform services, these keys are provided in the Command Data Field of APDU command and sent into the module electronically in plaintext which is allowed in FIPS 140-2 Security Level 2 according to FIPS 140-2 IG 7.7.

From the module's perspective, it does not support manual entry for keys, PINs and other CSPs.

In addition, the module does not output keys/CSPs, except the RSA public key, or their intermediate values in plaintext format outside its physical boundary.

7.4 Key Storage, Protection, and Destruction

The module stores the keys mentioned below in the Flash memory of the embedded Smart Card chip (i.e., on-chip Flash memory). Data in the Flash memory is protected by the secure design of the Smart Card chip.

Depending on how the UniMate Token is initialized, it may include any or all of the following keys:

- Authentication Keys and Data Encryption Keys: Issue Key, External Authentication Key, Internal Authentication Key, Maintenance Key, Master Key, User PIN, Admin PIN, PIN Unblock Key, PIN Reload Key

- Data Encryption Keys: Triple-DES key, AES key

- Digital Signature Keys: RSA public and private key pairs

Keys may be loaded into the UniMate Token during the initialization at factory. Keys may also be added or changed by the Issuer or Admin roles upon authentication. The symmetric key and RSA key pairs may be generated within the token or imported into the token by the User role.

The following table lists all keys that can possibly be present in a UniMate Token:

Key/CSP Name	**Details**
Issue Key	**Usage:** Ensure security of token initialization and the access rights of the issuer. **Accessible by Roles:** Issuer Role **Type:** 168-bit Triple-DES **Generation/Input:** Externally generated, entered in plaintext form in factory. Can be changed by Issuer Role. **Output:** Never exits the module **Storage:** Stored in plaintext in MF **Zeroization:** Cannot be deleted but can be changed upon Issuer Role authentication
Master Key	**Usage:** Create file/write key (if a file specifies the Master Key to be the file encryption key) **Accessible by Roles:** All roles **Type:** 168-bit Triple-DES **Generation/Input:** Externally generated, entered in plaintext in factory or by the Issuer Role **Output:** Never exits the module **Storage:** Stored in plaintext in files with ID 00 00 **Zeroization:** Can be deleted and zeroized by calling FORMAT DEVICE APDU command upon Issue Role authentication
Admin PIN	**Usage:** Authenticate Admin Role **Accessible by Roles:** Admin Role

Key/CSP Name	Details
	Type: 8-24 alphanumeric characters converted to a 24-byte binary string with appropriate padding **Generation/Input:** Externally generated, entered in plaintext form in factory or by Admin Role **Output:** Never exits the module **Storage:** Stored in plaintext in the files with ID 00 00 **Zeroization:** Can be deleted and zeroized by calling FORMAT DEVICE APDU command upon Issuer Role authentication
User PIN	**Usage:** Authenticate User Role **Accessible by Roles:** User Role **Type:** 8-24 alphanumeric characters converted to a 24-byte binary string with appropriate padding **Generation/Input:** Externally generated, entered in plaintext in factory, by Admin Role or User Role **Output:** Never exits the module **Storage:** Stored in plaintext in Files with ID 00 00 **Zeroization:** Can be deleted and zeroized by calling FORMAT DEVICE APDU command upon Issuer Role authentication
External Authentication Key	**Usage:** UniMate authenticates an external entity **Accessible by Roles:** All roles **Type:** 168-bit Triple-DES key **Generation/Input:** Externally generated, entered in plaintext in factory or by Admin Role **Output:** Never exits the module **Storage:** Stored in plaintext in files with ID 00 00 **Zeroization:** Can be deleted and zeroized by calling FORMAT DEVICE APDU command upon Issuer Role authentication
Internal Authentication Key	**Usage:** UniMate is authenticated to an external entity **Accessible by Roles:** All roles **Type:** 168-bit Triple-DES key **Generation/Input:** Externally generated, entered in plaintext in factory or by Admin Role **Output:** Never exits the module **Storage:** Stored in plaintext in files with ID 00 00 **Zeroization:** Can be deleted and zeroized by calling FORMAT DEVICE APDU command upon Issuer Role authentication
PIN Unblock Key	**Usage:** Unblock a locked User PIN

Key/CSP Name	Details
	Accessible by Roles: Admin Role **Type:** 168-bit Triple-DES key **Generation/Input:** Externally generated, entered in plaintext in factory or by Admin Role **Output:** Never exits the module **Storage:** Stored in plaintext in files with ID 00 00 **Zeroization:** Can be deleted and zeroized by calling FORMAT DEVICE APDU command upon Issuer Role authentication
PIN Reload Key	**Usage:** Reset User PIN **Accessible by Roles:** Admin Role **Type:** 168-bit Triple-DES key **Generation/Input:** Externally generated, entered in plaintext in factory or by Admin Role **Output:** Never exits the module **Storage:** Stored in plaintext in files with ID 00 00 **Zeroization:** Can be deleted and zeroized by calling FORMAT DEVICE APDU command upon Issuer Role authentication
Maintenance key	**Usage:** Used for the calculation of CMAC of data transit in APDU commands **Accessible by Roles:** Admin Role **Type:** 168-bit Triple-DES key **Generation/Input:** Externally generated, entered in plaintext in factory or by Admin Role **Output:** Never exits the module **Storage:** Stored in plaintext in files with ID 00 00 **Zeroization:** Can be deleted and zeroized by calling FORMAT DEVICE APDU command upon Issuer Role authentication
128-, 192- and 256-bit AES keys	**Usage:** Used for data encryption and decryption **Accessible by Roles:** User Role **Type:** AES Key **Generation/Input:** Internally generated using DRBG, or externally generated and then imported into the token via the data field of the Command APDU **Output:** Never output from the UniMate token **Storage:** Stored in files with ID in the form of 0E XX, where XX ranges from 00 to 7F **Zeroization:** Can be deleted and zeroized by calling DELETE FILE APDU command upon User

Key/CSP Name	Details
	authentication, or by calling FORMAT DEVICE APDU command upon Issuer Role authentication
168-bit Triple-DES key	**Usage:** Used for data encryption and decryption **Accessible by Roles:** User Role **Type:** Triple-DES Key **Generation/Input:** Internally generated using DRBG, or externally generated and then imported into the token via the data field of the Command APDU **Output:** Never output from the UniMate token **Storage:** Stored in files with ID in the form of 0E XX, where XX ranges from 00 to 7F **Zeroization:** Can be deleted and zeroized by calling DELETE FILE APDU command upon User authentication, or by calling FORMAT DEVICE APDU command upon Issuer Role authentication
2048-bit RSA Public key	**Usage:** RSA signature verification **Accessible by Roles:** User Role **Type:** RSA public key **Generation/Input:** Internally generated using DRBG and RSA key pair generation, or externally generated and then imported into the token via the data field of the Command APDU **Output:** The internally generated RSA public keys may be output from the token via the data field of the Response APDU by calling READ BINARY APDU command. **Storage:** Stored in files with ID in the form of 1E YY, where YY ranges from 00 to 7F **Zeroization:** Can be deleted and zeroized by calling DELETE FILE APDU command upon User authentication, or by calling FORMAT DEVICE APDU command upon Issuer Role authentication
2048-bit RSA Private key	**Usage:** RSA signature generation **Accessible by Roles:** User Role **Type:** RSA private key **Generation/Input** Internally generated using DRBG and RSA key pair generation, or externally generated and then imported into the token via the data field of the Command APDU **Output:** Never output from the UniMate token **Storage:** Stored in files with ID in the form of 1E ZZ,

Key/CSP Name	Details
	where ZZ ranges from 80 to FF **Zeroization:** Can be deleted and zeroized by calling DELETE FILE APDU command upon User authentication, or by calling FORMAT DEVICE APDU command upon Issuer Role authentication
CTR_DRBG CSPs	**Usage:** Random number generation whose output can be further used for symmetric key or asymmetric key generation **Accessible by Roles:** The CSPs in the internal state of DRBG are not accessible to any roles **Type:** AES Key and entropy input **Generation/Input:** Entropy input is from on-chip hardware-based NDRNG. The AES key is included in the binary of the firmware. **Output:** The resulting random bit strings may be output from the token via the data field of the Response APDU. **Storage:** The AES key is part of the binary of the firmware stored in the on-chip Flash memory. The entropy input is stored in the on-chip RAM. **Zeroization:** The CSPs in the internal state of DRBG are zeroized upon power off.

Table 8: Keys Present in Token

Zeroization is performed automatically at the end of the functions that the keys are presented in the APDU commands. It is done by filling the memory area with zeros or other values immediately before the completion of an APDU command call and re-establishing the connection between the module and the host.

8. EMI/EMC

The module meets the requirements of 47 CFR PART 15 regulation & ANSI C63.4 and ICES-003 for the evaluation of Class B of electromagnetic compatibility. This device complies with Part 15 of FCC Class B rules for home or office use, with FCC ID: 2ABTZUNIMATETOKEN and FCC test report number: R2BJ140211050-00.

9. Self-Tests

The UniMate USB/TRRS PKI Token implements a number of self-tests to ensure the proper functioning of the module. This includes power-up self-tests and conditional self-tests.

The power-up self-tests can be initiated by inserting the UniMate USB/TRRS PKI Token into a USB port of a host or TRRS audio port of a mobile device. The token performs power-up self-tests automatically without operator intervention. If the self-tests passes, the “Success!” message is displayed on the LCD screen. If any of self-tests fail, an error message associated with the type of error is displayed on the LCD screen and the module enters into an infinite loop to prevent any further operation.

Upon the successful completion of self-tests, the token becomes operational. If any of the conditional self-tests fail, the token enters the error state and returns an error code to indicate the module entered error state. Once the module is in the error state, no cryptographic service is available and no data output is possible from the token. No APDU command can be executed in the error state. Operator can unplug the token from the host PC or mobile device and reconnect it to recover from the error state.

In addition, when the module is performing self-tests, no APDU commands can be processed and no data output is possible until self-tests are successfully completed.

The on-demand self-tests can be invoked by the Self-Test Command APDU to perform all the power-up self-tests.

9.1. Power-Up Tests

Whenever the power-up self-tests are initiated, the token performs the integrity test and the cryptographic algorithm Known Answer Test (KAT). If any self-test does not match the known answers value, these self-tests fail and the token enters into an error state.

9.1.1. Integrity test

The UniMate USB/TRRS PKI Token uses HMAC-SHA-1 for the integrity test of its firmware.

9.1.2. Cryptographic algorithm KAT

Upon power-up, a KAT is performed for the following FIPS-Approved algorithms:

- AES encryption and decryption tested separately in ECB and CBC mode with 128-, 192- and 256-bit key size
- Triple-DES encryption and decryption tested separately in ECB and CBC mode with 168-bit key size

- RSA signature generation and verification tested separately with 2048-bit key and SHA-224
- SP800-90A CTR_DRBG with 128-bit AES key
- SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512
- CMAC with 3-key Triple-DES key

9.2. Conditional Tests

9.2.1. Pair-wise consistency test

The UniMate USB/TRRS PKI Token performs the pair-wise consistency test for each pair of RSA keys that it generates. The consistency of the key pair is tested by first calculating and then verifying a digital signature. The token uses the RSA private key for signature generation and its corresponding public key for signature verification.

9.2.2. Continuous random number generation test

The UniMate USB/TRRS PKI Token implements a continuous random number generation test for the DRBG based on NIST SP800-90A. The UniMate implements a block cipher DRBG, CTR_DRBG, which generates a minimum of 128-bit of random value per request. The random data generated for every request is compared with the data generated from the previous request. If the generated data for two requests are identical, a conditional test error flag is raised. For the first request made to any instantiation of the SP800-90A DRBG implemented in the token, two internal cycles to generate two bytes of random value are compared.

The UniMate USB/TRRS PKI Token also implements a continuous random number generation test for the non-Approved RNG HW RNG. The HW RNG generates 128-bit of random value per request, which is the entropy input to the FIPS-Approved CTR_DRBG. The 16 bytes of data generated for every request is compared with the 16 bytes of data generated from the previous request. If the generated data for two requests are identical, a conditional test error flag is raised. For the first request made to any instantiation of the HW RNG implemented in the module, two internal cycles to generate two 16 bytes of random value are compared.

10. Design Assurance

10.1. Configuration Management

The UniMate USB/TRRS PKI Token development team utilizes Visual SVN, a software versioning and revision control system, to maintain the current and historical versions of files such as source code and design documentation that contribute to the formation of the module.

Visual SVN integrates several aspects of the software development process in a distributed development environment to facilitate project-wide coordination of development activities across all phases of the product development life cycle:

- Configuration Management – the process of identifying, managing, and controlling software modules as they change over time
- Version Control – the storage of multiple versions of a single file along with details about each version
- Change Control – centralizes the storage of files and controls changes to files through the process of checking files in and out

The list of files that are relevant to the UniMate USB/TRRS PKI Token and is subject to Subversion control have been provided by SecuTech to the test laboratory.

10.2. Guidance and Secure Operation

This section describes how to configure the module for FIPS-Approved mode of operation. Operating the module without maintaining the following settings will remove the module from the FIPS-Approved mode of operation.

10.2.1. Cryptographic officer guidance

The initial Issue Key must be delivered to the Issuer in a secure manner (e.g., in a sealed envelope via a trusted carrier).

The Issuer must change the Issue Key as soon as the tokens are received. The Issuer must initialize the on-Card File System by creating necessary key files and loading needed Authentication Keys/PINs, in accordance to the guidance given in “UniMate USB/TRRS PKI Token Card Operating System Manual.” The detailed initialization procedures are described in the dedicated document, “UniMate USB/TRRS PKI Token Quick Guide.”

The Issuer must deliver the Authentication Keys/PINs to the Admin in a secure manner and request the Admin to change the default Authentication Keys/PINs as needed before the first use of the token.

10.2.2. User guidance

As soon as the correctly initialized UniMate token reaches the end-user, the user shall choose a strong PIN with at least 8 characters and use it to replace the default User PIN immediately.

11. Mitigation of Other Attacks

No other attacks are mitigated.

12. Abbreviations

AES	Advanced Encryption Specification
APDU	Application Protocol Data Unit and is the standard logical packet to communicate with a smartcard
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CFS	on-Card File System
CLA	Instruction class in a command APDU indicates the type of command
CMVP	Cryptographic Module Validation Program
COS	on-Card Operating System
CSP	Critical Security Parameter
CST	Cryptographic Services Testing
DES	Data Encryption Standard
DF	Dedicated File in a smart card file structure, equivalent to an intermediate directory
DRBG	Deterministic Random Bit Generator
EF	Elementary File in a smart card file structure, equivalent to a file
FIPS	Federal Information Processing Standards

FSM	Finite State Model
GPC	General Purpose Computer
GUI	Graphic User Interface
HMAC	Hash Message Authentication Code
IEC	International Electronic Commission
INS	Instruction code in a command APDU indicates the specific command
ISO	International Standard Organization
KAT	Known Answer Test
Lc	The number of bytes of command data in a command APDU to follow
Le	The maximum number of response bytes to expected after a command APDU
MAC	Message Authentication Code
MF	Master File in a smart card file structure, equivalent to the root directory of a file system
NIST	National Institute of Science and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
OE	Operational Environment
OFB	Output Feedback
O/S	Operating System
P1, P2	Instruction parameters for a command APDU
PCB	Printed Circuit Board
RNG	Random Number Generator
RSA	Rivest, Shamir, Addleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SW1,SW2	Status words in a response APDU indicates the command processing status
TDES	Triple-DES
TRRS	Tip-Ring-Ring-Sleeve
USB	Universal Serial Bus
CCID	Circuit(s) Cards Interface Device

13. References

[1] FIPS 140-2 Standard, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[2] FIPS 140-2 Implementation Guidance, http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf

[3] FIPS 140-2 Derived Test Requirements, http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402DTR.pdf

[4] FIPS 197, Advanced Encryption Standard (AES), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[5] FIPS 180-4 Secure Hash Standard, http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

[6] FIPS 186-4, Digital Signature Standard, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[7] NIST SP 800-67 Revision 1, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, http://csrc.nist.gov/publications/nistpubs/800-67-Rev1/SP-800-67-Rev1.pdf

[8] NIST SP 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf

[9] NIST SP 800-131A Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf

[10] ISO/IEC 7816 Integrated circuit(s) cards with contacts