Advanced Card Systems Ltd.

AET63 BioTRUSTKey

REFERENCE MANUAL

Version 1.8 09-2006

Unit 1008, 10th Floor, Hongkong International Trade and Exhibition Centre
1 Trademart Drive, Kowloon Bay, Hong Kong
Tel: +852 2796 7873 Fax: +852 2796 1286 Email: info@acs.com.hk Website: www.acs.com.hk

Contents

1. Introduction

The AET63 BioTRUSTKey is an interface for the communication between a computer (for example, a PC), a smart card and TFM (Trusted Fingerprint Module). Different types of smart cards have different commands and different communication protocols. This prevents, in most cases, the direct communication between a smart card and a computer. The AET63 BioTRUSTKey establishes a uniform interface from the computer to the smart card for a wide variety of cards. By taking care of the card specific particulars, it releases the computer software programmer of getting involved with the technical details of the smart card operation, which are in many cases not relevant for the implementation of a smart card system.

The AET63 BioTRUSTKey is connected to the computer through USB interface. The reader accepts commands from the computer, carries out the specified function at the smart card and returns the requested data or status information.

2. Features

- ISO7816-1/2/3 compatible smart card interface
- Enrolls fingerprint, encrypts into fingerprint template and stores inside smart card
- Retrieves fingerprint template from smart card and verifies the fingerprint template inside the AET63
- Supports CPU-based cards with T=0 and/or T=1 protocol
- Support PPS (Protocol and Parameters Selection) with 9600 – 96000 bps in reading and writing smart cards
- USB interface to PC with simple command structure
- Security application modules (SAM) inside the reader supporting CPU-based cards with T=0 and/or T=1 protocol (SAM Reader only)

3. Supported Card Types

The AET63 can operate MCU card with T=0 and T=1 protocol. The table presented in Appendix A explains which card type selection value must be specified for the various card types supported by the reader.

3.1 Microcontroller-based smart cards (asynchronous interface)

The AET63 supports EEPROM microcontroller-based cards with internal programming voltage (VPP) generation and the following programming parameters transmitted in the ATR:

PI1 = 0 or 5
I = 25 or 50

The AET63 performs the Protocol and Parameters Selection (PPS) procedure as specified *in ISO7816-3:1997*.

When the card ATR indicates the specific operation mode (TA_2 present; bit b5 of TA_2 must be 0) and that particular mode is not supported by the AET63, the reader will reset the card to set it to negotiable mode. If the card cannot be set to negotiable mode, the reader will reject the card.

When the card ATR indicates the negotiable mode (TA_2 not present) and communication parameters other than the default parameters, the AET63 will execute the PPS and try to use the communication parameters that the card suggested in its ATR. If the card does not accept the PPS, the reader will use the default parameters (F=372, D=1).
For the meaning of the aforementioned parameters, please refer to *ISO7816, part 3*.

4. Smart Card Interface

The interface between the AET63 and the inserted smart card follows the specifications of *ISO7816-3* with certain restrictions or enhancements to increase the practical functionality of the AET63.

4.1 Smart Card Power Supply VCC (C1)

The current consumption of the inserted card must not be higher than **50mA**.

4.2 Programming Voltage VPP (C6)

According to ISO 7816-3, the smart card contact C6 (VPP) supplies the programming voltage to the smart card. Since all common smart cards in the market are EEPROM based and do not require the provision of an external programming voltage, the contact C6 (VPP) has been implemented as a normal control signal in the AET63. The electrical specifications of this contact are identical to those of the signal RST (at contact C2).

4.3 Card Type Selection

The controlling PC has to always select the card type through the proper command sent to the AET63 prior to activating the inserted MCU card.

For MCU-based cards the reader allows to select the preferred protocol, T=0 or T=1. However, this selection is only accepted and carried out by the reader through the PPS when the card inserted in the reader supports both protocol types. Whenever an MCU-based card supports only one protocol type, T=0 <u>or</u> T=1, the reader automatically uses that protocol type, regardless of the protocol type selected by the application.

4.4 Interface for Microcontroller-based Cards

For microcontroller-based smart cards only the contacts C1 (VCC), C2 (RST), C3 (CLK), C5 (GND) and C7 (I/O) are used. A frequency of 4 MHz is applied to the CLK signal (C3).

4.5 Card Tearing Protection

The AET63 provides a mechanism to protect the inserted card when it is suddenly withdrawn while it is powered up. The power supply to the card and the signal lines between the AET63 and the card are immediately deactivated when the card is being removed. As a general rule, however, to avoid any electrical damage, **a card should only be removed from the reader while it is powered down.**

NOTE - The AET63 does never by itself switch on the power supply to the inserted card. This must explicitly be done by the controlling computer through the proper command sent to the reader.

5. Power Supply

The AET63 requires a voltage of 5V DC, 100mA, regulated, power supply. The AET63 gets the power supply from PC (through the cable supplied along with each type of reader).

Status LEDs

Two green LED on the front of the reader indicates the activation status of the smart card interface and the status of power supply of the device:

First Green LED - Indicates power supply to the device, i.e., the device is receiving power from the computer. As long as the device is connected to the PC, this LED light is on.

Second Green LED – Indicates that a smart card is present in the device, i.e., the smart card is activated. As long as there is a smart card inserted in the device, this light is on.

NOTE – This is applicable if you are using the PCSC device installer for AET63

6. USB Interface

The AET63 is connected to a computer through a USB following the USB standard.

6.1 Communication Parameters

The AET63 is connected to a computer through USB as specified in the USB Specification.

The AET63 is working in low speed mode, i.e. 1.5 Mbps.

USB Interface Wiring

Pin	Signal	Function
1	**V_{BUS}**	+5V power supply for the reader
2	**D-**	Differential signal transmits data between AET63 and PC.
3	**D+**	Differential signal transmits data between AET63 and PC.
4	**GND**	Reference voltage level for power supply

NOTE - In order for the AET63 to function properly through USB interface, either ACS proprietary device drive or ACS PC/SC device driver has to be installed. Please refer to the *Device Driver Installation Guide* for more detail.

7. Communication Protocol

In the normal operation, the AET63 acts as a slave device with regard to the communication between a computer and the reader. The communication is carried out in the form of successive command-response exchanges. The computer transmits a command to the reader and receives a response from the reader after the command has been executed. A new command can be transmitted to the AET63 only after the response to the previous command has been received.

There are two cases where the reader transmits data without having received a command from the computer, namely, the Reset Message of the reader and the Card Status Message.

7.1 Command

7.1.1 Normal Command (Length < 255 bytes)

A command consists of four protocol bytes and a variable number of data bytes and has the following structure:

Byte	1	2	3	4 ... N+3 (0<N<255)	N+4
	Header	Instruction	Data length = N	Data	Checksum

Header 01_H to indicate the start of a standard command.

02_H to indicate the start of an encrypted command (support from firmware 0.67 onwards, only used in PTVerifySC(*) and PTVerifySCAll(*))

Instruction The instruction code of the command to be carried out by the AET63

Data Length Number of subsequent data bytes.(0 < N < 255)

Data Data contents of the command.

For a READ command, for example, the data bytes would specify the start address and the number of bytes to be read. For a WRITE command, the data bytes would specify the start address and the data to be written to the card.

The data bytes can represent values to be written to a card and/or command parameters such as an address, a counter, etc.

Checksum The checksum is computed by XORing all command bytes including header, instruction, data length and all data bytes.

Note (*) : Please refer to “BioTRUSTKey API Manual.doc” for the descriptions of PTVerifySC and PTVerifySCAll.

The following example shows the structure of a command with instruction code = 91_H and three data bytes with the values 11_H, 22_H and 33_H, respectively:

byte	1	2	3	4	5	6	7
	01_{H}	91_{H}	03_{H}	11_{H}	22_{H}	33_{H}	93_{H}

7.1.2 Extended Command

A command consists of six protocol bytes and a variable number of data bytes and has the following structure:

byte	1	2	3	4	5	6 ... N+5 (N>0)	N+6
	Header	Instruction	Data Length = N			Data	Checksum
			FF_{H}	Data Length N			

Header 01_{H} to indicate the start of a standard command.

02_{H} to indicate the start of an encrypted command (support from firmware 0.67 onwards, only used in PTVerifySC$^{(*)}$ and PTVerifySCAll$^{(*)}$)

Instruction The instruction code of the command to be carried out by the AET63.

Data Length Number of subsequent data bytes, and is encoded in 3 bytes. The first byte is FF_{H}. The second byte and the third byte represent data length N.

Data Data contents of the command.

For a READ command, for example, the data bytes would specify the start address and the number of bytes to be read. For a WRITE command, the data bytes would specify the start address and the data to be written to the card.

The data bytes can represent values to be written to a card and/or command parameters such as an address, a counter, etc.

Checksum The checksum is computed by XORing all command bytes including header, instruction, data length and all data bytes.

Note (*) : Please refer to "BioTRUSTKey API Manual.doc" for the descriptions of PTVerifySC and PTVerifySCAll.

7.2 Response

The response from the AET63 to any command depends on whether the command has been received by the reader without error (e.g., checksum error).

7.2.1 No transmission error with normal response (Length < 255 bytes)

The response by the AET63 to a correctly received command consists of three protocol bytes, two status bytes and a variable number of data bytes and has the following structure:

byte	1	2	3	4	5 ... N+4 (0<N<255)	N+5
	Header	SW1	SW2	Data length = N	Data	Checksum

Header 01_H to indicate the start of the normal response.

02_H to indicate the start of an encrypted response (support from firmware 0.67 onwards, only used in PTVerifySC(*) and PTVerifySCAll(*))

SW1 Indicates the command execution status:

90_H = command successfully executed

60_H = error in command data; command cannot be executed

67_H = error detected in command execution

FF_H = status message initiated by the reader

SW2 Further qualification of the command execution status.

A table listing the possible values of the status bytes SW1 and SW2 and the corresponding meaning is given in Appendix B.

Data Length Number of subsequent data bytes (0 < N < 255)

Data Data contents of the command.

For a *READ_DATA* command, for example, the data bytes would contain the contents of the memory addresses read from the card. The data bytes can represent values read from the card and/or status information.

Checksum The checksum is computed by XORing all response bytes including header, status bytes, data length and all data bytes.

Note (*) : Please refer to “BioTRUSTKey API Manual.doc” for the descriptions of PTVerifySC and PTVerifySCAll.

The following example shows the structure of the response to a command which has successfully been executed and which returns three data bytes with the values 11_H, 22_H and 33_H, respectively:

byte	1	2	3	4	5	6	7	8
	01_H	90_H	00_H	03_H	11_H	22_H	33_H	92_H

7.2.2 No transmission error with extended response

The response by the AET63 to a correctly received command consists of three protocol bytes, two status bytes and a variable number of data bytes and has the following structure:

byte	1	2	3	4	5	6	7 ... N+6 (N>0)	N+7
	Header	SW1	SW2	Data length = N			Data	Checksum
				FF_H	Data Length N			

Header 01_H to indicate the start of the normal response.

02_H to indicate the start of an encrypted response (support from firmware 0.67 onwards, only used in PTVerifySC(*) and PTVerifySCAll(*))

SW1 Indicates the command execution status:

90_H = command successfully executed

60_H = error in command data; command cannot be executed

67_H = error detected in command execution

FF_H = status message initiated by the reader

SW2 Further qualification of the command execution status.

A table listing the possible values of the status bytes SW1 and SW2 and the corresponding meaning is given in Appendix B.

Data Length Number of subsequent data bytes, and is encoded in 3 bytes. The first byte is FF_H. The second byte and the third byte represent data length N.

Data Data contents of the command.

For a *READ_DATA* command, for example, the data bytes would contain the contents of the memory addresses read from the card. The data bytes can represent values read from the card and/or status information.

Checksum The checksum is computed by XORing all response bytes including header, status bytes, data length and all data bytes.

Note (*) : Please refer to “BioTRUSTKey API Manual.doc” for the descriptions of PTVerifySC and PTVerifySCAll.

7.2.3 Transmission error

If the receiving party of a command (i.e., the AET63) or a response (i.e., the computer) detects an error in the data length or the checksum of a command, it disregards the received data and sends a "NOT ACKNOWLEDGE" message to the transmitting party upon completion of the faulty transmission. The "NOT ACKNOWLEDGE" message consists of two bytes:

byte	1	2
	05_H	05_H

If the AET63 responds with a 'NOT ACKNOWLEDGE' message to a command from the computer, the computer would normally transmit the command again. If the computer detects a transmission error in a response from the AET63, it can send the 'NOT ACKNOWLEDGE' to the reader upon which the reader will transmit the most recent response again.

7.3 Card Status Message

When a card is being inserted into the reader or an inserted card is being removed from the reader while the reader is idle, i.e., not executing a command, the reader transmits a Card Status Message to notify the host computer of the change in the card insertion status.

In a system where these unsolicited messages from the reader to the computer are not desired, they can be disabled with the *SET_NOTIFICATION* command. Please note that the setting made with this command is volatile and will be lost with the next reader reset or power up. By default, the Card Status Message will be transmitted by the reader after a reset.

The Card Status Messages have the following structure and contents:

Card Status Message for Card Insertion

byte	1	2	3	4	5
	Header	**SW1**	**SW2**	**Data length**	**Checksum**
	01_H	FF_H	01_H	00_H	FF_H

Card Status Message for Card Removal

byte	1	2	3	4	5
	Header	**SW1**	**SW2**	**Data length**	**Checksum**
	01_H	FF_H	02_H	00_H	FC_H

A card status message is transmitted only **once** for every card insertion or removal event. The reader does not expect an acknowledge signal from the computer. After transmitting a status message, the reader waits for the next command from the computer.

NOTE - If the card is being removed from the reader **while a card command is being executed**, the reader will transmit a normal response to the computer with the response status bytes indicating the card removal during command execution (see *Appendix B: Response Status Codes*).

7.4 Transmission Protocol

The start of a command (to the reader) or a response (from the reader, including the Reset Message and Card Status Messages) is indicated by the respective party through the transmission of the single byte Start-of-Text (STX) character with the value 02_H.

The end of a command or response is indicated through the single byte End-of-Text (ETX) character with the value 03_H.

Within the command and response transmission only ASCII characters representing the hexadecimal (hex) digits 0...F are used. Each byte of a command or response is split into its upper and lower halfbyte (nibble). For each halfbyte is transmitted the ASCII character representing the respective hex digit value. For example, to transmit the data byte $3A_H$, two bytes are actually sent on the interface, namely, 33_H (ASCII code for '3') followed by 41_H (ASCII code for 'A'):

Data byte value	$3A_H$	
Transmitted values	33_H = '3'	41_H = 'A'

The following example shows the transmission of a command with instruction code $A2_H$ and one data byte with the value $3D_H$. The command has the following structure:

byte	1	2	3	4	5
	Header	**Instruction**	**Data length**	**Data**	**Checksum**
	01_H	$A2_H$	01_H	$3D_H$	$9F_H$

This command is transmitted on the serial interface in 12 bytes as follows:

byte	1	2	3	4	5	6	7	8	9	10	11	12
	STX	**'0'**	**'1'**	**'A'**	**'2'**	**'0'**	**'1'**	**'3'**	**'D'**	**'9'**	**'F'**	**ETX**
	02_H	30_H	31_H	41_H	32_H	30_H	31_H	33_H	44_H	39_H	46_H	03_H

For the representation of the hex halfbyte values as the corresponding ASCII characters in commands, the AET63 accepts both upper case characters 'A' ... 'F' (41_H ... 46_H) and lower case characters 'a' ... 'f' (61_H ... 66_H):

byte	1	2	3	4	5	6	7	8	9	10	11	12
	STX	**'0'**	**'1'**	**'A'**	**'2'**	**'0'**	**'1'**	**'3'**	**'D'**	**'9'**	**'F'**	**ETX**
	02_H	30_H	31_H	41_H	32_H	30_H	31_H	33_H	44_H	39_H	46_H	03_H

... is equivalent to:

byte	1	2	3	4	5	6	7	8	9	10	11	12
	STX	**'0'**	**'1'**	**'a'**	**'2'**	**'0'**	**'1'**	**'3'**	**'d'**	**'9'**	**'f'**	**ETX**
	02_H	30_H	31_H	61_H	32_H	30_H	31_H	33_H	64_H	39_H	66_H	03_H

In its response messages, the AET63 uses upper case characters 'A' ... 'F'.

8. COMMANDS

The commands executed by the AET63 can generally be divided into two categories, namely, Control Commands and Card Commands.

Control Commands manage the internal operation of the AET63. They do not directly affect the card inserted in the reader and are therefore independent of the selected card type.

Card Commands are directed toward the card inserted in the AET63. The structure of these commands and the data transmitted in the commands and responses depend on the selected card type.

8.1 Control Commands

8.1.1 GET_ACR_STAT

This command returns relevant information about the particular AET63 model and the current operating status, such as, the firmware revision number, the maximum data length of a command and response, the supported card types, and whether a card is inserted and powered up.

Command format

Instruction Code	Data length
01 H	00 H

Response data format

<table>
<tr><th colspan="10">INTERNAL</th><th>MAX_C</th><th>MAX_R</th><th colspan="2">C_TYPE</th><th>C_SEL</th><th>C_STAT</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

INTERNAL 10 bytes data for internal use only

MAX_C The maximum number of command data bytes.

MAX_R The maximum number of data bytes that can be requested to be transmitted in a response.

C_TYPE The card types supported by the AET63. This data field is a bitmap with each bit representing a particular card type. A bit set to '1' means the corresponding card type is supported by the reader and can be selected with the *SELECT_CARD_TYPE* command. The bit assignment is as follows:

byte	1								2							
card type	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

See Appendix A for the correspondence between these bits and the respective card types.

C_SEL The currently selected card type as specified in a previous *SELECT_CARD_TYPE* command. A value of 00_H means that no card type has been selected.

C_STAT Indicates whether a card is physically inserted in the reader and whether the card is powered up:

00_H : no card inserted

01_H : card inserted, not powered up

03_H : card powered up

8.1.2 SELECT_CARD_TYPE

This command sets the required card type. The firmware in the AET63 adjusts the communication protocol between reader and the inserted card according to the selected card type.

Command format

Instruction Code	Data length	Data
		TYPE
02_H	01_H	

TYPE See Appendix A for the value to be specified in this command for a particular card to be used.

Response data format

No response data

8.1.3 RESET

This section describes the *RESET* command only for the case when no card type is selected or when the card type 00_H is selected. For all other cases, please refer to the specific section described for each individual card type.

Command format

Instruction Code	Data length
80_H	00_H

Response data format

ATR			

ATR The answer-to-reset string returned by the card.

The return status code for this command is 90 00_H when the inserted card is a T=0 card, 90 01_H when the inserted card is a T=1 card, and 90 10_H when the inserted card is a memory card; otherwise the status code is 60 20_H.

8.1.4 SET_NOTIFICATION

This command disables / enables the Card Status Messages transmitted by the reader to notify the host computer of the insertion or removal of a card.

Command format

Instruction Code	Data length	Data
		NOTIFY
06_H	01_H	

NOTIFY Specifies whether the Card Status Message shall be transmitted to notify the host computer of card insertion / removal

01_H : transmit Card Status Message

02_H : do not transmit Card Status Message

Response data format

No response data

8.1.5 SET_OPTION

This command selects the options for the reader.

Command format

Instruction Code	Data length	Data
		Option
07_H	01_H	

Option Bit 0 (LSB bit): Select for PPS mode

Specifies reader ⇔ card communication speed

0 : baud rate to/from the card is from 9600 bps to 96000 bps (default)

1 : baud rate to/from the card is at 9600 bps only

Bit 2 : Select smart card file type for storing fingerprint template

0 : transparent file type (default)

1 : record file type

Bit 4 : Select for EMV mode

Specifies whether the reader is in EMV mode

0 : reader not in EMV mode (default)

1 : reader in EMV mode

Bit 7 : Select for TFM mode

Specifies whether to access TFM in intercept or transparent mode

0 : Intercept mode (default)

1 : Transparent mode

Reserved

Response data format

No response data

8.2 EEPROM Commands

8.2.1 EEPROM_READ_DATA

This command is used to read the specified number of bytes from the specified address of the EEPROM.

Command format

Instruction Code	Data length	Data		
		ADDR		LEN
$9A_H$	03_H			

ADDR Byte address of first byte to be read from the EEPROM. The high byte of the address is specified as the first byte of ADDR.

LEN Number N of data bytes to be read from the EEPROM

(0 < N ≤ MAX_R)

Response data format

BYTE 1	BYTE 2	BYTE 3	...	...	BYTE N

BYTE x Data bytes read from the EEPROM memory

8.2.2 EEPROM_WRITE_DATA

This command is used to write the specified data bytes to the specified address of the EEPROM.

Note: The EEPROM used in AET63 is 24C512, with a page size of 64 bytes. The page write and page alignment are not done in the firmware, and these should be done in the driver or application.

Command format

Instruction Code	Data length	Data					
	LEN	ADDR		BYTE 1	...	...	BYTE N
$9B_H$							

LEN Number of data bytes to be written to the EEPROM, N, + 2

ADDR Byte address in the EEPROM of the first byte to be written. The high byte of the address is specified as the first byte of ADDR.

BYTE x Byte values to be written to the EEPROM starting at address ADDR. BYTE 1 is written to address ADDR; BYTE N is written to address ADDR+N-1.

Response data format

No response data

8.3 *TFM (Trusted Fingerprint Module) Commands*

8.3.1 TFM_COMMAND

This command is used to send the command to the TFM.

Command format

Instruction Code	Data length	Data				
	LEN	TFM Command				
9C $_H$			…	…	…	

LEN Number N of command to be sent to the TFM

(0 < N ≤ MAX_R)

DATA The TFM command (please refer to TFM API Documentation)

Response data format

BYTE 1	BYTE 2	BYTE 3	...	...	BYTE N

BYTE x Data bytes returned by the TFM (please refer to TFM API Documentation)

8.3.2 TFM_RESET

This command resets the TFM and then waits for the ATR returned from the TFM.

Command format

Instruction Code	Data length
9D $_H$	00 $_H$

Response data format

ATR					

ATR Answer-To-Reset as transmitted by the TFM. Please refer to the TFM Communication Protocol for the ATR format.

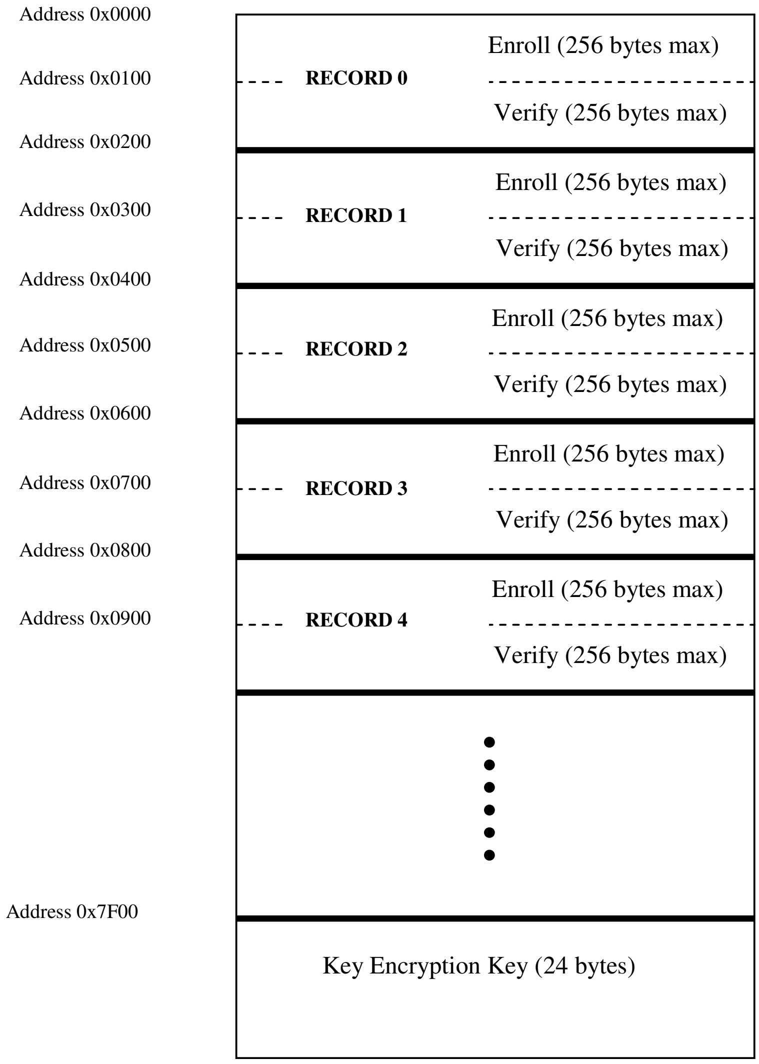
8.3.3 TFM_SMARTCARD

This is used to get list of APDUs from the EEPROM and then send the APDUs to the smart card. The list of APDUs selects the correct file in the smart card for the enrollment or verification of the fingerprint template.

Command format

Instruction Code	Data length	Data	
	LEN	ADDR	
9E $_H$	02 $_H$		

ADDR Address of the EEPROM stores the list of APDUs. Please refer to the "Application Notes for Handling Fingerprint Template in AET63" for detailed information



Response data format

No response data

8.3.4 TFM_OPEN_SECURE_SESSION

This command sends 24 bytes of random number to AET63. The random number is used to general the session key.

Command format

Instruction Code	Data length	Data				
	LEN			…..		
$9F_H$	18_H			…..		

Data 24 bytes of random number to generate the session key

Response data format

No response data

8.4 MCU-based Card

8.4.1 RESET

This command powers up the card inserted in the card reader and performs a card reset. If the card is powered up when the command is being issued, only a reset of the card is carried out. The power supply to the card is not switched off.

Command format

Instruction Code	Data length
80_H	00_H

Response data format

ATR					

ATR Answer-To-Reset as transmitted by the card according to ISO7816-3.

NOTE - The ATR is only returned in the AET63 response if the communication protocol of the card is compatible with the reader, i.e., if the card can be processed by the AET63. Otherwise, the AET63 returns an error status and deactivates the smart card interface.

8.4.2 POWER_OFF

This command powers off the card inserted in the card reader.

Command format

Instruction Code	Data length
81_H	00_H

Response data format

No response data

8.4.3 EXCHANGE_APDU

To exchange an APDU (Application Protocol Data Unit) command/response pair between the MCU card inserted in the AET63 and the host computer.

Command format

Instruction Code	Data length	Data									
	LEN	CLA	INS	P1	P2	Lc	BYTE 1	...2	...	BYTE N	Le
$A0_H$											

LEN Length of APDU command data, N, + 6 $(0 < N \le MAX\_R)$

CLA APDU instruction class byte

INS APDU instruction

P1 APDU parameter byte 1

P2 APDU parameter byte 2

Lc APDU command data length

BYTE x APDU command data

Le Expected APDU response data length (Le = 0 means no data is expected from the card)

NOTE - With the T=0 communication protocol it is not possible to transmit data to the card and from the card in a single command-response pair. Hence, only either Lc or Le can be greater than 0 in an *EXCHANGE_APDU* command when a T=0 card is in the reader. If both parameters have a value greater than 0, the AET63 does not execute the command and returns an error status.

Response data format

BYTE 1	...	...	BYTE N	SW1	SW2

BYTE x Response data from card (if any)

SW1, SW2 Status code returned by the card.

8.4.4 EXCHANGE_T1_FRAME

To exchange an APDU (Application Protocol Data Unit) command/response pair between the MCU card inserted in the AET63 and the host computer using T1 protocol.

Command format

Instruction Code	Data length	Data
	LEN	T1 BLOCK FRAME
A1 $_H$		

LEN Length of APDU command data, N

DATA T1 Block frame to be sent to the card

Response data format

BYTE 1	...	...	BYTE N

BYTE x Response T1 Block from card (if any)

8.5 Security Application Module (SAM)

Note: The commands in this section ACITIVATE_SAM, DEACTIVATE_SAM, EXCHANGE_SAM_APDU and EXCHANGE_SAM_T1_FRAME can only be used in SAM reader.

8.5.1 ACTIVATE_SAM

This command is used to power up and reset the specified SAM and transmit the SAM's ATR in the response.

Command format

Instruction Code	Data length	Data
		SM#
88_H	01_H	

SM# Must be 0; reserve for future use

Response data format

ATR					

ATR Answer-To-Reset as transmitted by the card according to ISO7816-3.

NOTE - The ATR is only returned in the AET63 response if the communication protocol of the SAM is compatible with the reader, i.e., if the SAM can be processed by the AET63. Otherwise, the AET63 returns an error status and deactivates the SAM.

8.5.2 DEACTIVATE_SAM

This command powers off the SAM

Command format

Instruction Code	Data length
89_H	00_H

Response data format

No response data

8.5.3 EXCHANGE_SAM_APDU

To exchange an APDU (Application Protocol Data Unit) command/response pair between the SAM card inserted in the AET63 and the host computer.

Command format

Instruction Code	Data length	Data									
	LEN	CLA	INS	P1	P2	Lc	BYTE 1	...2	...	BYTE N	Le
B0_H											

LEN Length of APDU command data, N, + 6 (0 < N ≤ MAX_R)

CLA APDU instruction class byte

INS APDU instruction

P1 APDU parameter byte 1

P2 APDU parameter byte 2

Lc APDU command data length

BYTE x APDU command data

Le Expected APDU response data length (Le = 0 menas no data is expected from the card)

NOTE - With the T=0 communication protocol it is not possible to transmit data to the card and from the card in a single command-response pair. Hence, only either Lc or Le can be greater than 0 in an *EXCHANGE_SAM_APDU* command when a T=0 card is in the reader. If both parameters have a value greater than 0, the AET63 does not execute the command and returns an error status.

Response data format

BYTE 1	...	...	BYTE N	SW1	SW2

BYTE x Response data from card (if any)

SW1, SW2 Status code returned by the card.

8.5.4 EXCHANGE_SAM_T1_FRAME

To exchange an APDU (Application Protocol Data Unit) command/response pair between the SAM card inserted in the AET63 and the host computer using T1 protocol.

Command format

Instruction Code	Data length	Data
	LEN	T1 BLOCK FRAME
B1 H		

LEN Length of APDU command data, N

DATA T1 Block frame to be sent to the card

Response data format

BYTE 1	...	...	BYTE N

BYTE x Response T1 Block from card (if any)

Appendix A: Supported Card Types

The following table summarizes which values must be specified in the *SET_CARD_TYPE* command for a particular card type to be used, and how the bits in the response to the *GET_ACR_STAT* command correspond with the respective card types.

Cyber-mouse card type code	Card Type
00_H	Auto-select T=0 or T=1 communication protocol
$0C_H$	MCU-based cards with T=0 communication protocol
$0D_H$	MCU-based cards with T=1 communication protocol
$C0_H$	SAM cards with T=0 communication protocol (SAM Reader only)
$D0_H$	SAM cards with T=1 communication protocol (SAM Reader only)

Appendix B: Response Status Codes

The following table summarizes the possible status code bytes SW1, SW2 returned by the AET63:

SW1	SW2	Status
90	00	OK – command successfully executed
90	01	OK – using T=1 protocol (only in response to the RESET command)
90	10	OK – synchronous protocol is used (only in response to the RESET command). The exact card type should be selected by using the SELECT_CARD_TYPE command.
60	01	No card type selected
60	02	No card in reader
60	03	Wrong card type specified
60	04	Card not powered up; This status code is also returned in a response if the card was temporarily removed during a card access.
60	05	Invalid Instruction Code
60	20	Card failure
60	22	Short circuit at card connector
62	01	Secret code verify failed
67	01	Command incompatible with card type
67	02	Card address error
67	03	Data length error
67	04	Invalid length of response (with READ command)
67	05	Secret code locked
67	12	APDU command aborted (only MCU-based card using T=1 protocol); the command abortion may be caused by a card internal failure.

Appendix C: Technical Specifications

Device

AET63 BioTRUSTKey

Power supply

Power supply	USB powered
Supply voltage	Regulated 5V DC

Universal Serial Bus Interface

Type	USB v1.1, four lines: +5V, GND, D+ and D-
Power source	From USB
Speed	1.5 Mbps (Low Speed)

Smart Card Interface

Standard	ISO 7816 1/2/3, T=0 and T=1
Supply current	max. 50mA
Smart card read / write speed	9600 – 96000 bps
Short circuit protection	+5V / GND on all pins

The presence of the smart card power supply voltage is indicated through a green LED on the reader

CLK frequency	4 MHz
Card connector	Landing contacts (8 contacts)
Card insertion cycles	min. 100,000

Fingerprint Scanner Interface

Power consumption	Active mode : 20mA @ 5V + 105mA @ 3.3V Sleep mode :< 1mA @ 5V + 70µA @ 3.3V
Active sensor size	12.8 x 18 mm
Array size	256 x 360 pixels
Image resolution	508 DPI
ESD tolerant	+/- 15kV air discharge

Case

Color	Silver-gray

Operating Conditions

Temperature	0 - 50° C
Humidity	5% - 93%

Standard/Certifications

CE, FCC

OS

Windows 98, ME, NT4, 2K, XP and Linux

OEM

OEM-Logo possible, customer-specific colors

Note: This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

> **NOTE:** This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- □ Reorient or relocate the receiving antenna.
- □ Increase the separation between the equipment and receiver.
- □ Connect the equipment into an outlet on a circuit different from that to which the receiver is needed.
- □ Consult the dealer or an experienced radio/TV technician for help.