



BIOMODULE MOS

TECHNICAL SPECIFICATIONS

XSPC6N190
Revision 1.0

Copyright © 2006 id3 Semiconductors.

All rights reserved.

Due to continued product development this information may change without notice. If you find any problems in the documentation, please report them to us in writing. id3 Semiconductors does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying and recording or otherwise without the prior written permission of id3 Semiconductors.

id3 Semiconductors

5, rue de la Verrerie
F – 38120 Le Fontanil-Cornillon

Internet E-Mail: contact@id3semiconductors.com

Website: <http://www.id3semiconductors.com>

Revision History

Revision	Date	Author	Description
1.0	Jan 23, 2006	CC	First release.

Table of Contents

- 1. Introduction 7**
 - 1.1. Overview7
 - 1.2. Features7
 - 1.3. Description7
 - 1.4. Applications8
 - 1.5. References.....8
- 2. Functional Description..... 9**
 - 2.1. Overview9
 - 2.2. Typical Architecture9
 - 2.3. Biometric Operations.....10
- 3. Technical Description 12**
 - 3.1. Block Diagram.....12
 - 3.2. Dedicated Cryptographic and Imaging Processor 13
 - 3.3. Host Interface 13
 - 3.4. Auxiliary Input/Output 13
- 4. Biometric Specifications 14**
 - 4.1. Fingerprint Authentication Performance14
 - 4.2. Fingerprint Sensor Specifications15
- 5. Smart Card Specifications..... 16**
 - 5.1. Overview16
 - 5.2. Biometric User Cards17
 - 5.3. Biometric SAM.....17
- 6. Biometric System Description..... 19**
 - 6.1. Biometric System Credentials.....19
 - 6.2. Biometric Mechanisms.....19
 - 6.2.1. BioModule MOS Initialization19
 - 6.2.2. Biometric User Card Initialization19
 - 6.2.3. Biometric Enrollment20
 - 6.2.4. Fingerprint Deletion20
 - 6.2.5. Fingerprint Verification.....21
- 7. Electrical Specifications..... 22**
 - 7.1. Recommended Operating Conditions22
 - 7.2. Absolute Maximum Ratings22
 - 7.3. Electrical Characteristics.....23
 - 7.4. RESET Timing Requirements24
 - 7.5. Shutdown Timing Requirements24
 - 7.6. Module Standby25
 - 7.7. Module Boot sequence.....26
 - 7.8. Typical connection27
- 8. Mechanical Data 29**
 - 8.1. Recommended PCB layout29
 - 8.2. Board to board mounting.....29
 - 8.3. Package Mechanical Data.....30
 - 8.4. Fingerprint Sensor31
- 9. Evaluation and Development Kit..... 32**
 - 9.1. Overview32
 - 9.2. BioModule MOS Evaluation Board.....32
 - 9.3. Application Programming Interface33
 - 9.3.1. Communication Protocol.....33

9.3.2. BioModule API.....	33
9.3.3. Biometric Smart Card API.....	33
9.3.4. Documentation Support	34
9.4. AuthentIC Biometry Kit	34
10. Ordering Information	35
10.1. References.....	35
10.2. Contact us	35

List of Figures

Figure 1 : BioModule with flex and fingerprint sensor	7
Figure 2 : Typical architecture	9
Figure 3 : Fingerprint enrollment on smart card	10
Figure 4 : Fingerprint verification on smart card.....	11
Figure 5 : BioModule MOS Block Diagram	12
Figure 6 : Adjustable FAR (False Accept Rate)	14
Figure 7 : ROC curve	14
Figure 8 : High quality fingerprint image	15
Figure 9 : Biometric smart card architecture.....	16
Figure 10 : BioModule MOS Initialization	19
Figure 11 : Biometric User Card Initialization.....	20
Figure 12 : Fingerprint Enrollment	20
Figure 13 : Biometric Template Deletion	21
Figure 14 : Biometric Template Verification using BIO*Manager application.....	21
Figure 15 : RESET timing requirements	24
Figure 16 : Shutdown timing requirement.....	24
Figure 17 : Placing module in standby mode	25
Figure 18 : Resuming operation from standby mode.....	25
Figure 19 : Module boot sequence.....	26
Figure 20 : Typical connection	27
Figure 21 : Recommended PCB Layout	29
Figure 22 : Board to board mounting.....	29
Figure 23 : Package mechanical data (Top View)	30
Figure 24 : Package mechanical data (Bottom View)	30
Figure 25 : Fingerprint sensor mechanical data (AT77C101B-CB02)	31
Figure 26 : BioModule Evaluation Board.....	33

List of Tables

Table 1 : Pin assignments.....	12
Table 2 : Recommended Operating Conditions	22
Table 3 : Absolute Maximum Ratings	22
Table 4 : Electrical Characteristics	23
Table 5 : RESET timing requirement	24
Table 6 : Shutdown timing requirement	25
Table 7 : Wake up timing requirement.	26
Table 8 : Module boot sequence	26
Table 9 : Mechanical specifications	31
Table 10 : Ordering Information.....	35

1. Introduction

1.1. OVERVIEW

This document describes the specifications of id3 Semiconductors' BioModule MOS fingerprint recognition module.

1.2. FEATURES

- Highly secure architecture for code/data storage and processing
- Biometric operation with id3 Semiconductors Match-On-Smartcard technology
- Compliant with Oberthur Card Systems' ID-One Smart Cards
- High speed fingerprint verification (<1 second)
- Direct interfacing with Atmel FingerChip® fingerprint sensor.
- Asynchronous serial host interface
- Operates with a single 3.3V DC supply
- Low power consumption with advanced power management (< 0.5 μ A in shutdown mode).
- Operating temperature range : -10°C to +60°C
- Compact size (33mm x 23mm x 4mm)

1.3. DESCRIPTION

Based on Atmel's FingerChip fingerprint sensor, a dedicated cryptographic and imaging processor and Oberthur Card Systems' ID-One™ Smart Cards, the BioModule MOS provides the main biometric functions such as enrollment and authentication with Match-On-SmartCard in a package module, making it easy to integrate into a final system.

With "Match-On-Smartcard" technology, the fingerprint template and the matching algorithm are stored in the smart card itself preventing any crucial information from leaving the card and eliminating the possible concern of fingerprint database.

In addition to these features, the miniature sized module has a state-of-the-art low power design making it a perfect match in a wide range of applications from battery operated mobile equipments to network based security systems.

The BioModule MOS is particularly well-suited to physical access control, point of sales devices, or national ID card readers.

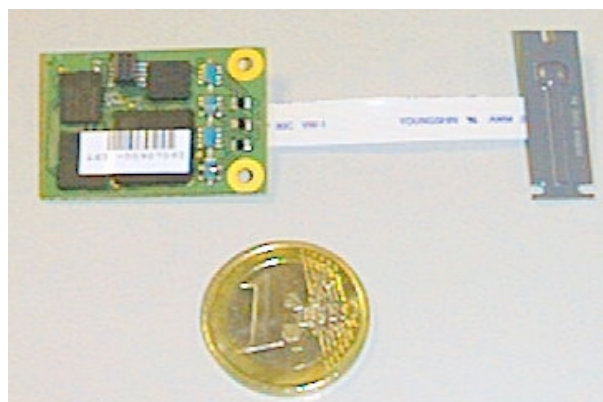


Figure 1 : BioModule with flex and fingerprint sensor

1.4. APPLICATIONS

- Logical/physical access control
- Time and attendance systems
- Portable points of sales
- National ID card readers
- Secure payment terminal

1.5. REFERENCES

The reader should refer to following references. id3 certifies that the present document complies with all referenced specifications, unless where expressly noted.

id3 Semiconductors

- [1] XSPC5J080 – BioModule Command Specifications
- [2] XSPC5K188 – BioModule Communication Protocol Software Stack Reference Guide
- [3] XSPC5K291 – BioModule Embedded Development Kit Documentation

Atmel

- [4] AT77C101B-FingerChip Datasheet

Oberthur Card Systems

- [5] AuthentIC-BIO Smartcard Application Reference Manual

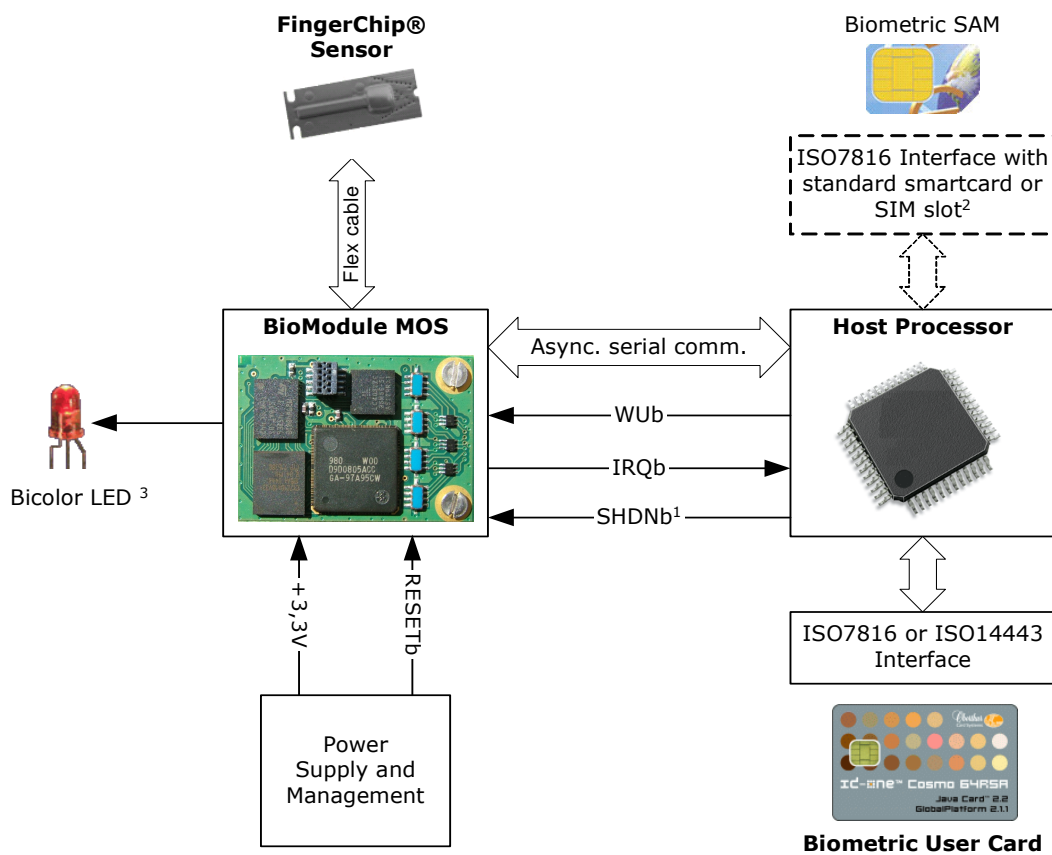
2. Functional Description

2.1. OVERVIEW

The BioModule MOS is a biometric sub-system based on Atmel's FingerChip fingerprint sensor and a dedicated cryptographic and imaging processor. Combined with Oberthur Card Systems' ID-One™ Smart Cards and Match-On-SmartCard technology, it offers the best possible performance and security for embedded system applications.

2.2. TYPICAL ARCHITECTURE

The BioModule MOS must be connected to a motherboard for power supplies and interface connections. The motherboard must have at least one smart card interface (contact ISO7816, contactless ISO14443, or USB). Optionally, if fingerprint enrollment is needed on the device, the motherboard should also be equipped with a second ISO7816 card interface and a SIM slot for a biometric SAM (Secure Access Module).



¹ Optional : only if deep power down is required.
² Optional : only if enrollment by the module is required. If not, enrollment can be done on PC using a BIOTHENTIC reader.
³ Optional : Bicolor LED shows biometric operation activities.

Figure 2 : Typical architecture

Secure Messaging

Communication between BioModule MOS and biometric smart cards (SAM or user card) uses state of art Triple-DES cryptography with authentication and encryption based on session keys.

The host processor is only a bridge between the BioModule MOS and the smart cards and is not able to the cryptograms exchanged.

2.3. BIOMETRIC OPERATIONS

The biometric module is used to perform the following operations:

Fingerprint enrollment on smart card

1. The end-user scans his fingerprint by sweeping it at least 4 times across the FingerChip sensor.
2. The BioModule MOS extracts a fingerprint signature reference (reference template) from the 4 images.
3. The motherboard gets an encrypted template from the BioModule and loads it into the smart card.

Note that the reference template is loaded under control of an administrator card (SAM).

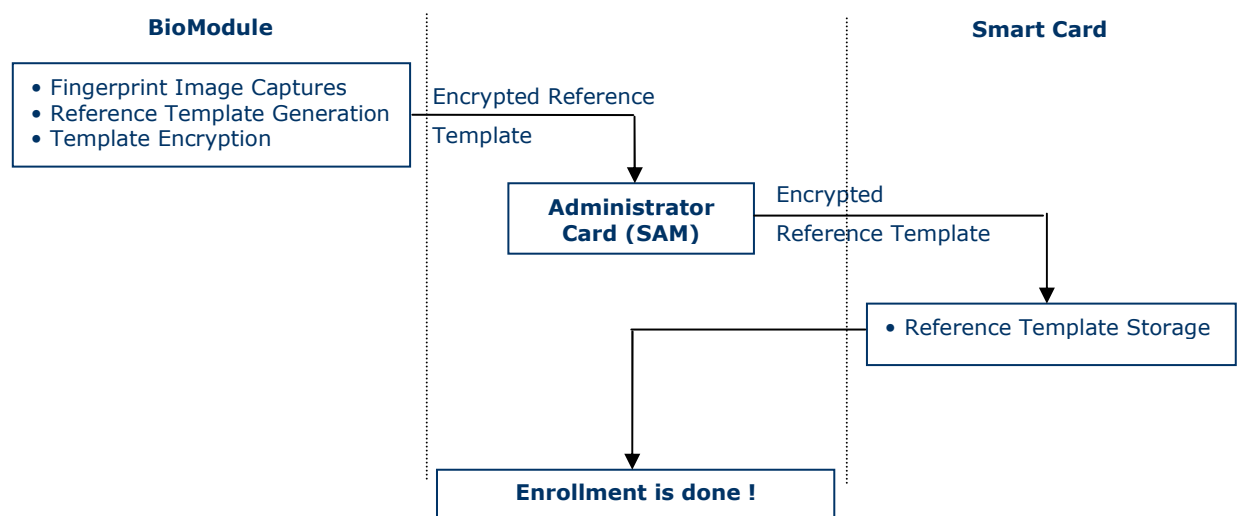


Figure 3 : Fingerprint enrollment on smart card

Fingerprint verification on smart card (Match-On-SmartCard)

1. The end-user scans his fingerprint by sweeping it across the FingerChip sensor.
2. The BioModule MOS extracts a fingerprint signature (candidate template) from the image.
3. The motherboard gets an encrypted template from the BioModule and sends it to the smart card.
4. The smart card performs matching of the candidate template against the reference template stored during the enrollment procedure.

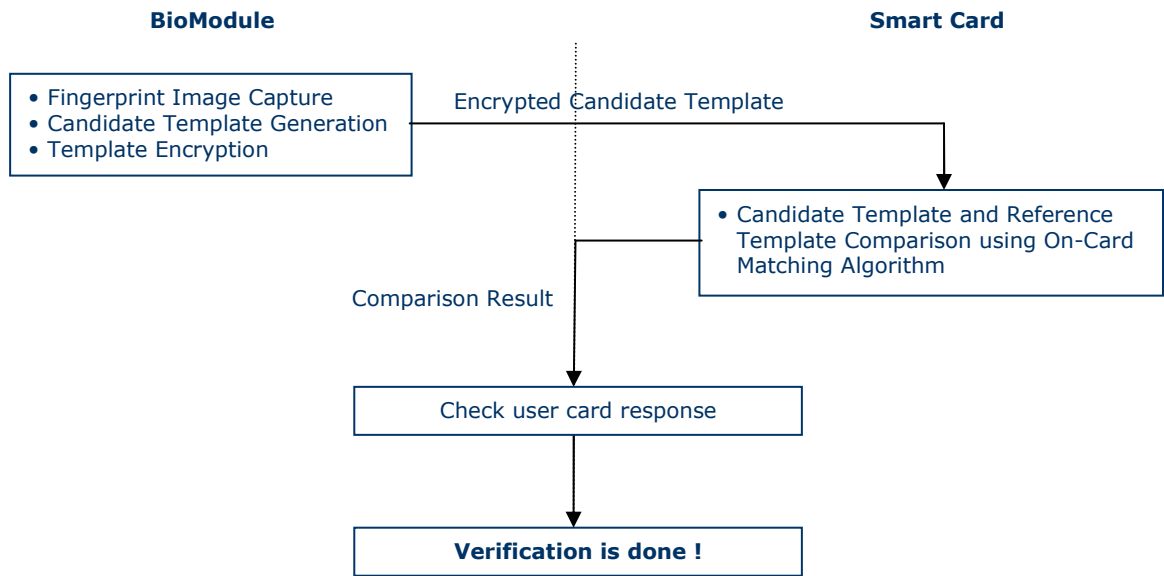


Figure 4 : Fingerprint verification on smart card

The BioModule Development Kit provides all the necessary tools and documentation to add these biometric operations to your products in a reduced development time.

3. Technical Description

3.1. BLOCK DIAGRAM

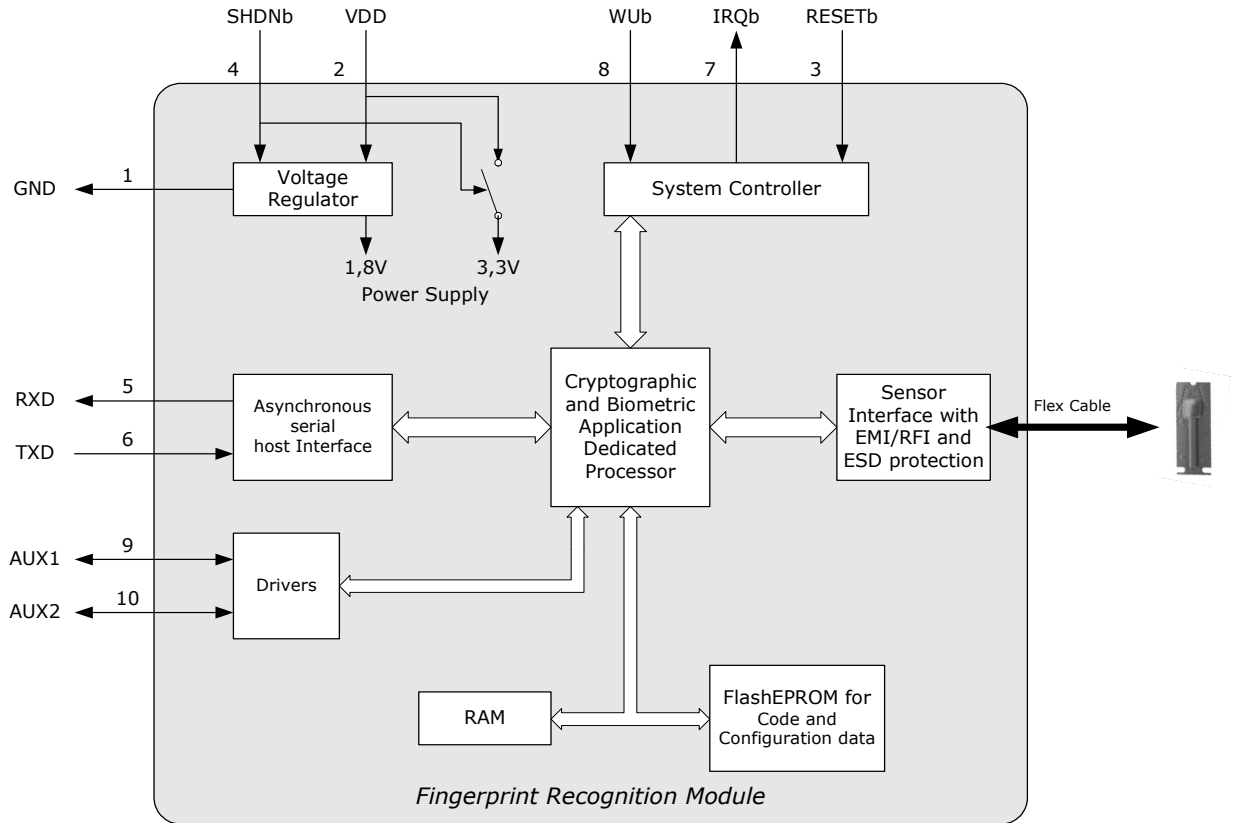


Figure 5 : BioModule MOS Block Diagram

Pin Assignments

Pin Number	Pin Name	Type	Description
1	GND	Power	Ground reference level
2	VDD	Power	Power supply
3	RESETb	Input	Device reset input
4	SHDNb	Input	Device shutdown
5	RXD	Input	Asynchronous data receive input
6	TXD	Output	Asynchronous data transmit output
7	IRQb	Output	Interrupt request open drain output
8	WUb	Input	Device wake up input (from standby mode)
9	AUX1	Input/Output	Auxiliary 1 input/output
10	AUX2	Input/Output	Auxiliary 2 input/output

Table 1 : Pin assignments

3.2. DEDICATED CRYPTOGRAPHIC AND IMAGING PROCESSOR

BioModule MOS is designed around a dedicated cryptographic and imaging processor. Thanks to its highly secure architecture, it's a perfect match with smart card security requirements.

Features

- Downloadable firmware after genuine code and data authentication.
- Handle image acquisition using ATMEL FingerChip™ sensor.
- High processing power and hardware image processing block.
 - Image treatment and template extraction in about 800ms.
- Cryptographic operations
 - Smartcard-like life cycle.
 - Key management and storage.
 - Secure channel management with smartcards.
 - Fully customizable security concept.

3.3. HOST INTERFACE

BioModule MOS provides a proprietary communication protocol for easy interface with most host systems thanks to an asynchronous serial host interface.

Description

- | | |
|--------------------------|-------------------------------------|
| ▪ Host communication | Asynchronous serial host interface |
| ▪ Baud rates | 115.2 kbps (optionally 38400 bauds) |
| ▪ Communication protocol | Proprietary (ID3NET) |

The BioModule Development Kit provides all the necessary tools and documentation to implement this communication protocol into an embedded application.

3.4. AUXILIARY INPUT/OUTPUT

BioModule MOS provides two auxiliary ports that may be independently configured as input, open drain output or push/pull output. They may be used for driving a bicolor LED for biometric activity (default behavior).

4. Biometric Specifications

4.1. FINGERPRINT AUTHENTICATION PERFORMANCE

The device's biometric performances are characterized by the following:

- EER (Equal Error Rate) < 0.5%
- FRR (False Reject Rate) < 2% (at FAR equal to 0.001%)
- FAR (False Accept Rate) < 0.001%, can be adjusted
- Enrollment time < 10 seconds (including 4 image captures)
- Matching time on smart card < 1 second (typ. 150 ms)
- Total verification time < 1 second
- Template size max. 256 bytes

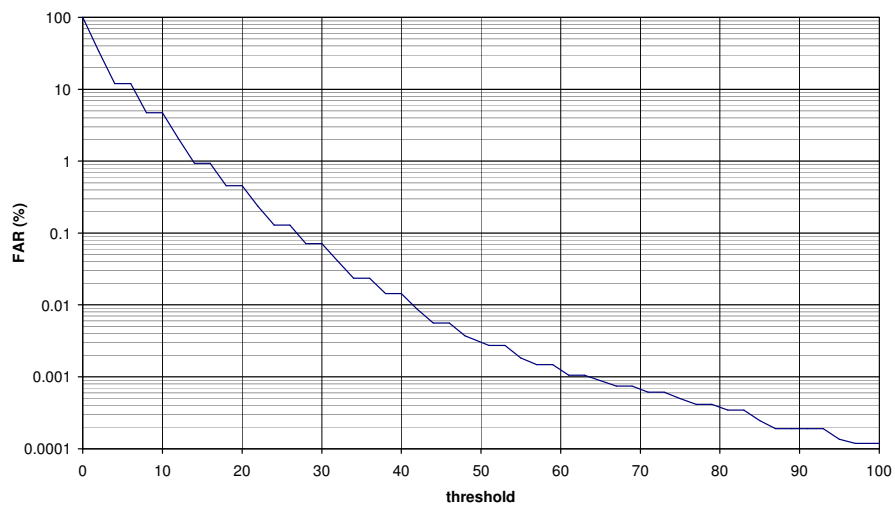


Figure 6 : Adjustable FAR (False Accept Rate)

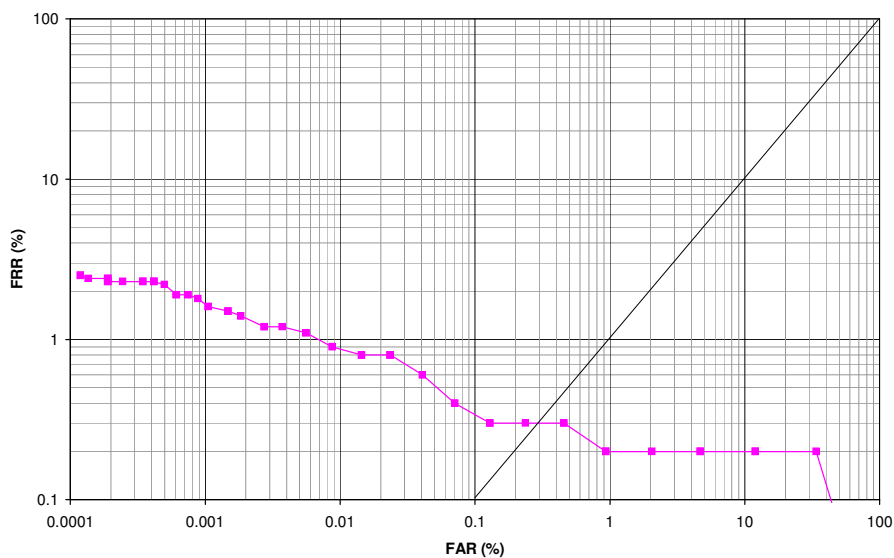


Figure 7 : ROC curve

4.2. FINGERPRINT SENSOR SPECIFICATIONS

BioModule MOS uses the FingerChip fingerprint sensor. The FingerChip's small size enables easy integration into the casing of the final product as opposed to rigid and larger sensors.

With its small and fully encapsulated sensing area, it also ensures maximum reliability and robustness over time. One need not worry about dirt, shocks, humidity or wide operating temperature ranges as with capacitive area sensors, the FingerChip being more highly protected against these stresses than any other sensor.

Description

- Manufacturer Atmel
- Device name Fingerchip® (AT77C101B-CB02 or AT77C102-CB02)
- Sensor technology Thermal, swiping type
- Sensing area 14.0mm x 0.4mm
- Image resolution 500 dpi
- Operating temperature range -30°C to +65°C
- Hard protective coating (made to withstand over 1 million swipes)
- Fully EMI/RFI and ESD protected sensor interface

Image Reconstruction Algorithm

BioModule MOS offers the best possible image quality thanks to an innovative reconstruction algorithm that minimizes image distortion due to approximate slice overlapping, and optimizes image contrast.

- Image distortion < 1%
- Finger swiping speed From 2 to 20 cm/s
- Final image size 300 x 428 pixels
- Gray levels 256



Figure 8 : High quality fingerprint image

5.2. BIOMETRIC USER CARDS

Description

The biometric user cards are loaded with the AuthentIC-BIO Smart Card application which implements a standard smartcard file system, and advanced cryptographic functionalities. The main access conditions (PIN or secure messaging) are enhanced with a cardholder authentication using fingerprint recognition. A dedicated applet is responsible for the management of the biometric templates (AuthentIC-Bio*Manager Application).

Features

- Provides asymmetric cryptographic facilities
- Provides biometric authentication methods
- Compliant with ISO 7816-4 file structures
- Compliant with ISO 7816-9 specification to provide dynamic file management
- Supports PKCS#15 to allow certificates management
- Adds fingerprint authentication to file access conditions

Access Conditions

The *File Access Conditions* are defined for each file as a set of rights to allow the issuance of a command on that file; an access condition is so the requested security level to be fulfilled prior to execute an operation.

There are two kinds of *File Access Conditions*:

- Credential verification :
 - Cardholder PIN (CHV),
 - Cardholder Biometric Data (BIO),
 - Security Officer PIN (SO),
 - Any combination of CHV, BIO and SO
- OP Authentication :
 - Plain Secure Channel
 - MACed Secure Channel
 - Encrypted/MACed Secure Channel

AuthentIC-Bio*Manager Application

The AuthentIC-BIO*Manager Smart Card application features a biometric manager that:

- Encapsulates all the proprietary information (sensitive or not) and mechanism used to implement biometrics as defined per Oberthur Card Systems and id3 Semiconductors,
- Provides biometric services (including biometric authentication of cardholder) to any applet through dedicated interfaces and shared instances.

5.3. BIOMETRIC SAM

Description

The biometric SAM, also called "Administrator card", is loaded with the AuthentIC-BIO*SAM application which provides cryptographic facilities in order to allow the personalization of biometric user cards as well as BioModule MOS fingerprint modules.

Features

- Enables BioModule MOS personalization before module deployment
- Enables user card personalization
- Enables user card administration (fingerprint enrollment, deletion, unlocking, etc.)

Credentials

The production commands are under control of the personalizer credential, meaning that the cardholder PIN or a biometric template – if available – must be verified prior to use them.

- Cardholder PIN or passphrase
- Biometric Data (up to ten fingerprint templates)

The enrollment of a fingerprint is performed under control of the cardholder PIN or a previously defined fingerprint template. The biometric templates are irreversibly locked after too many verification failures.

6. Biometric System Description

6.1. BIOMETRIC SYSTEM CREDENTIALS

Biometric Applicative Key

In order to allow the personalization of the BioModule MOS, the biometric SAM contains a 256-bit key (hereafter described as K_{AP}) used to export the biometric matching keys (see below) ciphered with a AES-CBC cipher.

Enrollment Master Key

In order to allow fingerprint enrollments on biometric cards (user cards or SAM), the biometric SAM defines an *Enrollment Master Key*, hereafter described as K_{ME} . This 128-bit DES key is diversified to compute the Diversified Enrolment Key, K_{E} , and used to decipher the enrollment data transmitted by the BioModule MOS.

Verification Master Key

In order to allow fingerprint verification on biometric cards (user cards or SAM), the biometric SAM defines a *Verification Master Key*, hereafter described as K_{MV} . This 128-bit DES key is diversified to compute the Diversified Enrolment Key, K_{V} , and used to decipher the biometric data transmitted by the BioModule MOS.

The *Verification Master Key* is loaded in an encrypted *Secure Channel* during personalization of the user cards. It is never possible to read or extract that key but it is possible to update it with a new value. The key is only used internally for biometric verification purposes

Biometric Card Administrative Key

In order to allow the authentication of the BIO*SAM application and of the enrollment officer, the biometric SAM shares a key with the biometric user cards. The reference data of this key are built from data defined by the BIO*SAM personalizer and by the enrollment officer. That *Biometric Card Administrative Key* is transmitted ciphered to the user card during the card initialization process and must later be verified by the AuthentIC-Bio application to allow additional enrollment as well as template deletion and unlocking.

6.2. BIOMETRIC MECHANISMS

6.2.1. BioModule MOS Initialization

The biometric SAM is used to initialize the applicative data of a BioModule MOS. The following scheme applies:

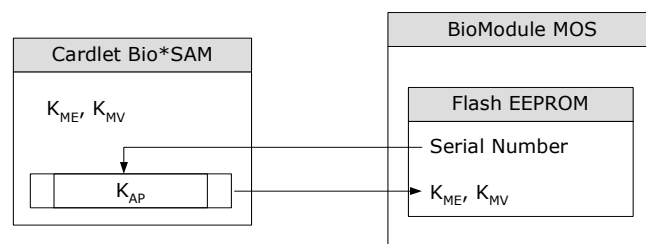


Figure 10: BioModule MOS Initialization

6.2.2. Biometric User Card Initialization

The Biometric User Cards need to be initialized before the first enrollment. During this process:

1. The BIO*SAM application establishes a *Secure Channel* with the AuthentIC-BIO*Manager application,
2. It transfers the K_{MV} key,
3. It creates the *Biometric Card Administrative Key* "Ka" onto the AuthentIC-BIO*Manager application,

All these credential transfers or creations use the facility of a *SM-DEC Secure Channel*, and thus all data are ciphered with the OP session keys.

The following scheme applies:

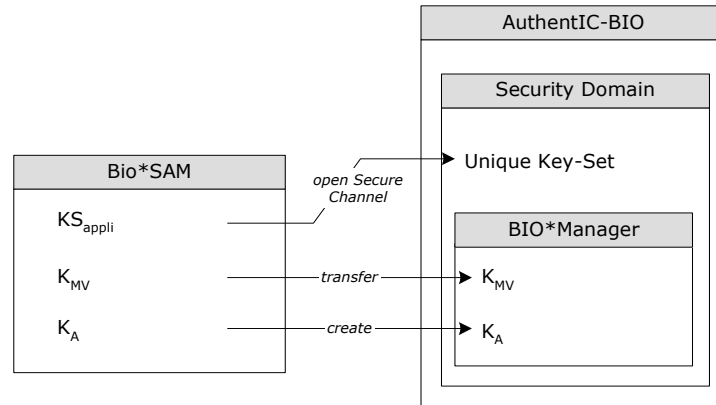


Figure 11: Biometric User Card Initialization

6.2.3. Biometric Enrollment

When a fingerprint enrollment is performed, the following processes occur:

1. The BIO*SAM application establishes a *Secure Channel* with the AuthentIC-BIO*Manager application,
2. It verifies the *Biometric Card Administrative Key* "Ka",
3. And finally it transfers the fingerprint information provided by the BioModule MOS.

The following scheme applies:

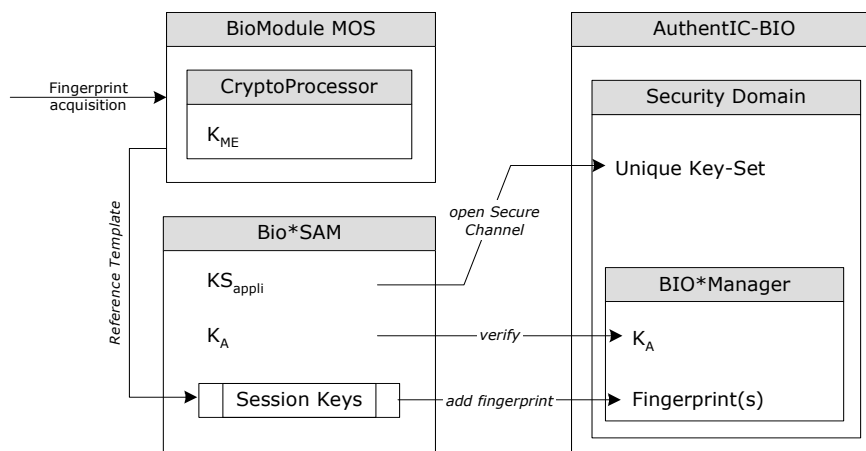


Figure 12: Fingerprint Enrollment

6.2.4. Fingerprint Deletion

When a biometric fingerprint is deleted, the following processes occur:

1. The BIO*SAM application establishes a *Secure Channel* with the AuthentIC-BIO*Manager application,
2. It verifies the *Biometric Card Administrative Key* "Ka",
3. And finally it transfers a delete fingerprint APDU command.

The following scheme applies:

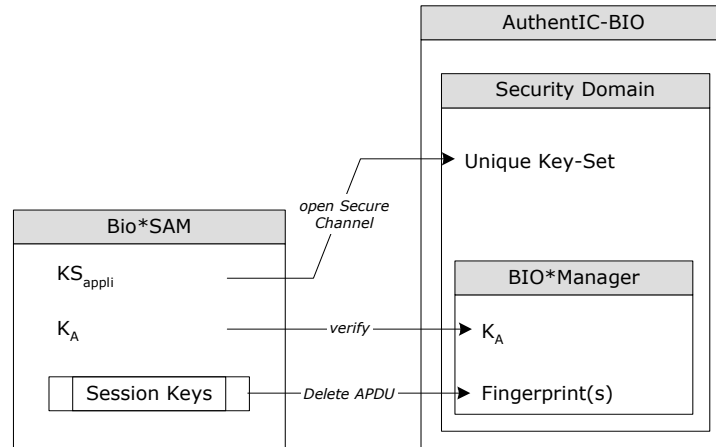


Figure 13: Biometric Template Deletion

6.2.5. Fingerprint Verification

When a fingerprint is verified, the following processes occur:

1. The reader crypto-processor transmits its unique identifier to the AuthentIC-BIO*Manager (or to another applet that uses the shared interface of the biometric manager)
2. It receives an unpredictable number from it;
3. It transfers the candidate fingerprint to the application.

One of the following schemes applies:

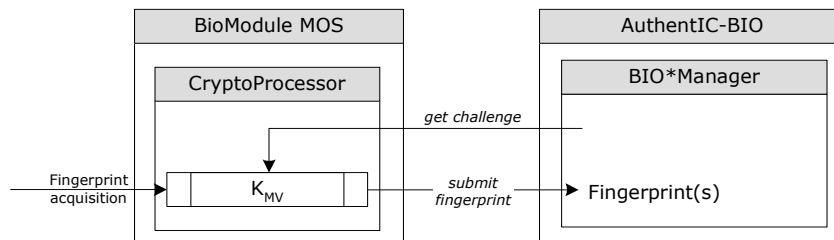


Figure 14: Biometric Template Verification using BIO*Manager application

7. Electrical Specifications

7.1. RECOMMENDED OPERATING CONDITIONS

Parameter	Test Conditions	Symbol	Min.	Typ	Max	Units
Supply voltage	Operating	V_{DD}	3.0	3.3	3.6	V
High-level input voltage (RXD, RESETb, WUb)		V_{IH}	2		$V_{DD} + 0.3$	V
Low-level input voltage (RXD, RESETb, WUb, SHDNb)		V_{IL}	-0.3		0.8	V
High-level output current (TXD)	Tested for V_{OH} min	I_{OH}			-2	mA
Low-level output current (TXD)	Tested for V_{OL} max	I_{OL}			2	mA
High-level output current (AUX1, AUX2) ¹	Tested for V_{OH} min	I_{OH}			-4	mA
Low-level output current (AUX1,AUX2,IRQb) ¹	Tested for V_{OL} max	I_{OL}			8	mA
Operating free-air temperature		T_a	-10		+60	°C

Table 2 : Recommended Operating Conditions

¹ Depending on device model, AUX1 and AUX2 may be configured as input or in output.

7.2. ABSOLUTE MAXIMUM RATINGS

Stress beyond those listed under Absolute Maximum Rating may cause permanent damage to the device. Exposure to absolute-maximum-rated conditions for extended periods may affect device reliability. All voltage values are with respect to GND.

Parameter	Symbol	Min.	Typ	Max	Units
Power supply voltage	V_{DD}	-0.3		4.0	V
Input voltage (RXD, RESETb, WUb)		-0.3		4.5	V
Input voltage (AUX1, AUX2) ¹		-0.5		5.5	V
Input voltage range (SHDNb)		-0.5		5.5	V
Output voltage (TXD)		-0.3		4.5	V
Output voltage (IRQb)		-0.5		5.5	V
Output voltage (AUX1, AUX2) ¹		-0.5		5.5	V
Storage temperature		-20		+85	°C

Table 3 : Absolute Maximum Ratings

¹ Depending on device model, AUX1 and AUX2 may be configured as input or in output.

7.3. ELECTRICAL CHARACTERISTICS

(Over recommended free-air temperature range)

Parameter	Test Conditions	Symbol	Min.	Typ*	Max	Units
Power consumption on VDD	Image acquisition with sensor heating	I_{DD1}		145	180	mA
Power consumption on VDD	Image acquisition with sensor not heating	I_{DD2}		70	90	mA
Power consumption on VDD	Executing command	I_{DD3}		50	70	mA
Power consumption on VDD	Waiting for command	I_{DD4}		35	40	mA
Power consumption on VDD	Standby mode	I_{DDstby}		5	7	mA
Power consumption on VDD	Shutdown mode ¹	I_{DDshdn}		<0.5	2	μA
Input current (RXD, WUb)	$GND < V_I < V_{DD}$	I_I	-5		5	μA
Input current (RESETb)	$GND < V_I < V_{DD}$	I_I	-7		7	μA
Input current (AUX1, AUX2) ²	$GND < V_I < V_{DD}$	I_I	-1		1	μA
Input current (AUX1, AUX2) ²	$V_{DD} < V_I < 5.5V$	I_I			10	μA
Pull up current (IRQb)	Open drain IRQb disabled	I_{PU}	-30		-150	μA
High-level output voltage (TXD)	$I_{OH} = -2mA$	V_{OH}	2.4			V
Low-level output voltage (TXD)	$I_{OL} = 2mA$	V_{OL}			0.4	V
High-level output voltage (AUX1, AUX2) ²	$I_{OH} = -4mA$	V_{OH}	2.4			V
Low-level output voltage (AUX1,AUX2,IRQb) ²	$I_{OL} = 8mA$	V_{OL}			0.4	V
Input capacitance (RXD, WUb)		C_I		5		pF
Input capacitance (RESETb)		C_I		20		pF
Input capacitance (AUX1, AUX2) ²		C_I		8		pF
Output capacitance (TXD)		C_O		5		pF
Output capacitance (IRQb)		C_O		8		pF

Table 4 : Electrical Characteristics

*All typical value are at $T_a = 25^\circ C$ and $V_{DD} = +3,3V$ unless otherwise noted.

¹ Care should be taken to place all device signals at GND level to prevent current flowing through pins.

² Depending on device model, AUX1 and AUX2 may be configured as input or in output.

7.4. RESET TIMING REQUIREMENTS

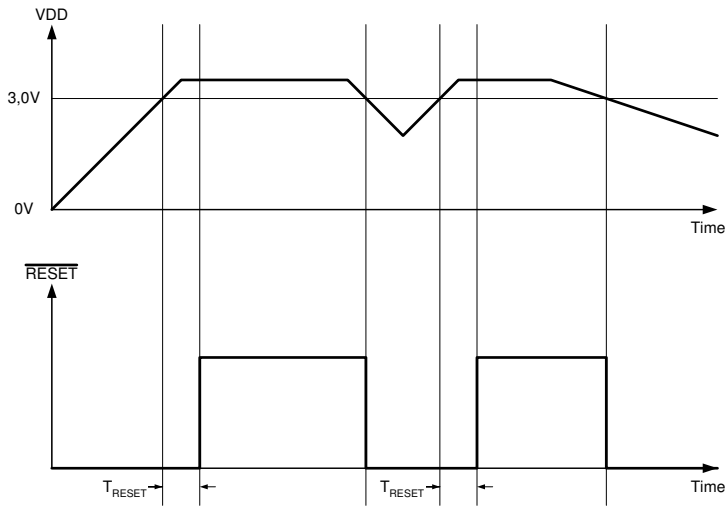


Figure 15 : RESET timing requirements

Parameter	Symbol	Min.	Typ	Max	Units
RESET pulse width	T_{RESET}	40			ms

Table 5 : RESET timing requirement

7.5. SHUTDOWN TIMING REQUIREMENTS

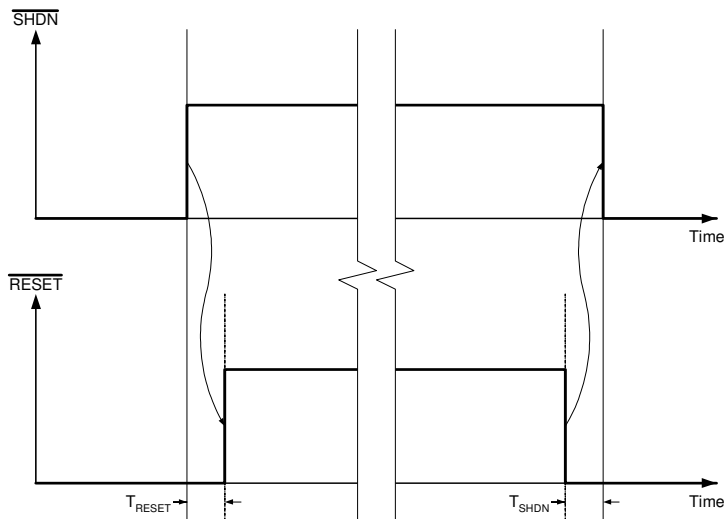


Figure 16 : Shutdown timing requirement

Parameter	Symbol	Min.	Typ	Max	Units
RESET pulse width after SHDN rising edge	T_{RESET}	40			ms
RESET assertion before SHDN falling edge	T_{SHDN}	0			ns

Table 6 : Shutdown timing requirement

7.6. MODULE STANDBY

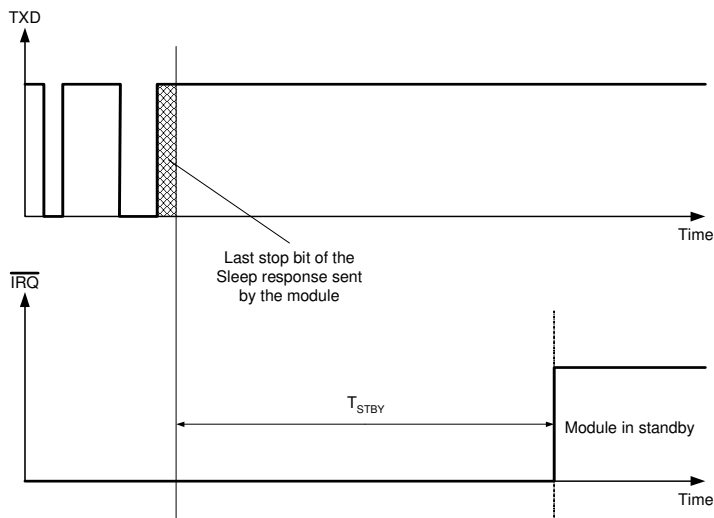


Figure 17 : Placing module in standby mode

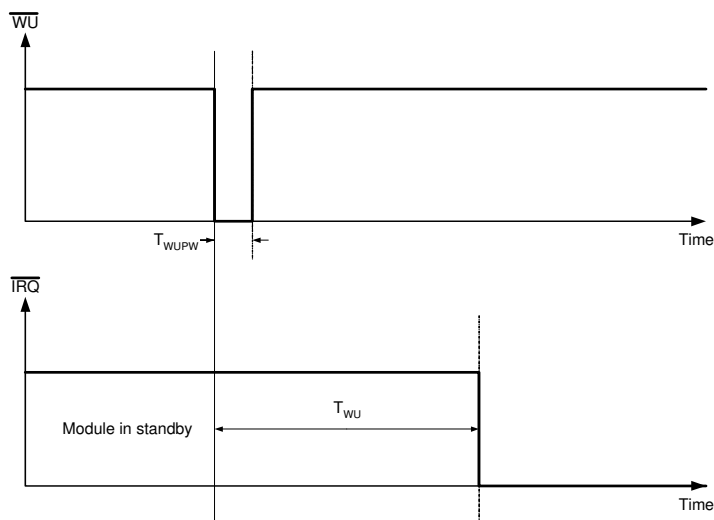


Figure 18 : Resuming operation from standby mode

Parameter	Symbol	Min.	Typ	Max	Units
Module en standby mode from response to Sleep command	T_{STBY}		10	15	ms
WU pulse width	T_{WUPW}	100			ns
Module wake up time from WU falling edge	T_{WU}		400	450	μ s

Table 7 : Wake up timing requirement.

7.7. MODULE BOOT SEQUENCE

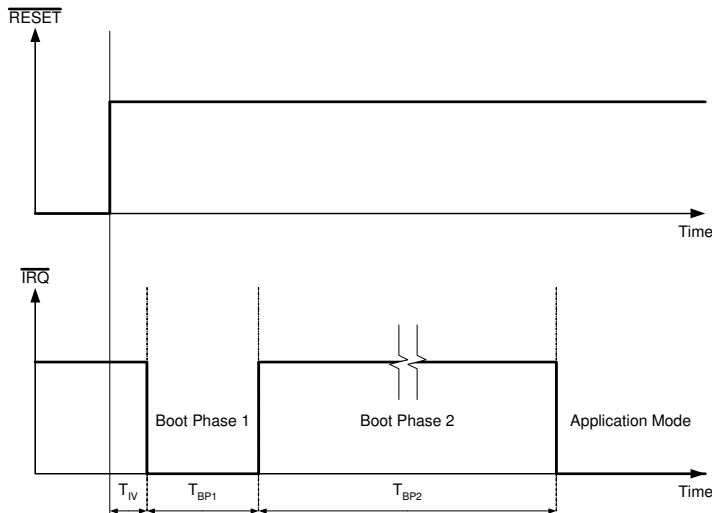


Figure 19 : Module boot sequence

Parameter	Symbol	Min.	Typ	Max	Units
IRQ valid from RESET rising edge	T_{IV}	0	32	40	μ s
Module Boot Phase 1	T_{BP1}	0	500	1000	ms
Module Boot Phase 2*	T_{BP2}		3	5	s

Table 8 : Module boot sequence

* Phase 2 may be drastically reduced by issuing a RUN command during this phase. RUN command can be issued immediately after phase 2 rising edge and will force the module to enter application mode immediately.

7.8. TYPICAL CONNECTION

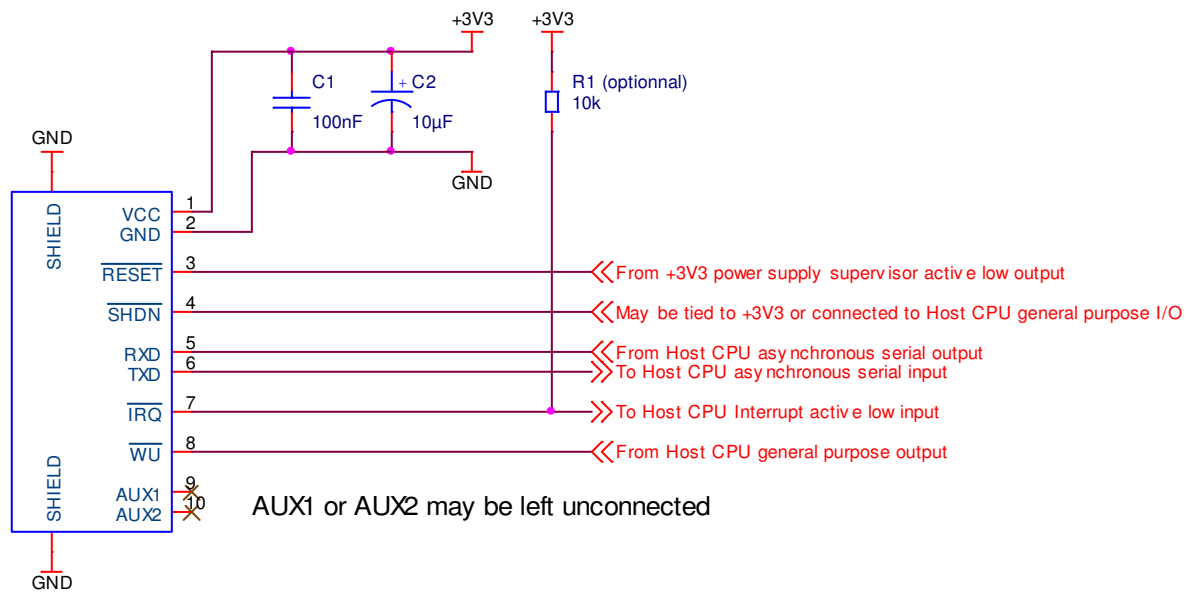


Figure 20 : Typical connection

Power Supply

Module power supply must be carefully decoupled using two capacitors. Recommended decoupling solution is a 100nF ceramic X7R type capacitor in parallel with a 10µF tantalum type capacitor placed as close as possible from the VCC pin of the module. See **Table 5 : RESET timing requirement**.

Active Low Shutdown input

Shutdown input allows host CPU to completely shutdown the module achieving the lowest module consumption. Putting this pin to low level removes power from internal module components. Therefore, designer must ensure that all others pins (RESET, RXD, TXD, IRQ, WU, AUX1 and AUX2) are also placed to low level to prevent current flowing through unpowered components. See **Table 6 : Shutdown timing requirement**.

Shield

The two holes provide also an electrical path to ground used to improve EMI/RFI shielding and ESD protection of the sensor. Designer must ensure the shortest path to ground using metal spacers to mount the module on the host board.

Active Low Reset input

Reset input is used to generate a global module reset. Designer must ensure that module is kept in RESET state whenever power supply voltage is out of specification. See **Table 5 : RESET timing requirement**.

Active Low Wake Up input

Wake Up input is used to get the module out of standby mode. The module is placed in standby mode by a command from host and is woken up by a low pulse on this pin. See **Table 7 : Wake up timing requirement**.

Active Low Interrupt output

Interrupt output is used by the module to trigger an interrupt request on the host CPU upon a software dependent event. The host CPU acknowledges the interrupt (the IRQ pin goes back to high level) by sending a command to the module. This pin is open drain and required a pull up. The module features a weak pull up of 47kOhms typical. Therefore, resistor R1 is optional and required only if a stronger pull up resistor is mandatory.

Auxiliary 1/2 input or output

Depending on module configuration, AUX1 and AUX2 may be independently configured as input, open drain output or push/pull output. They may be used for:

- Driving a bicolor LED for biometric activity (default behavior).
- WIEGAND DATA0/DATA1 or DATA/CLOCK output.

We may study any custom behavior upon customer request.

8. Mechanical Data

8.1. RECOMMENDED PCB LAYOUT

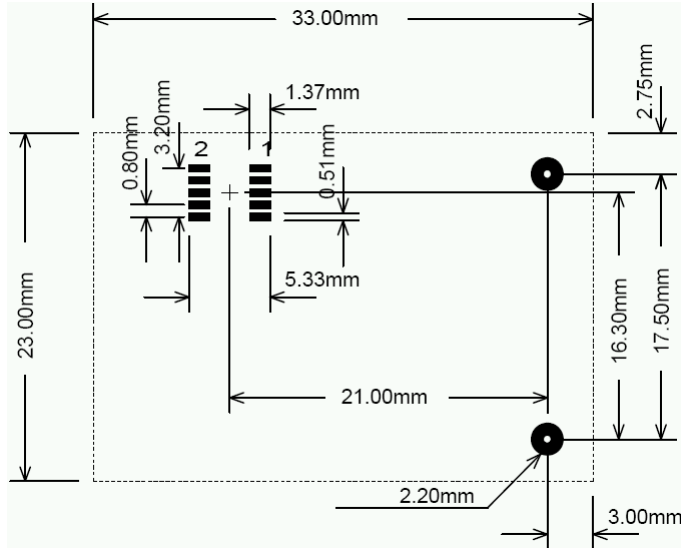


Figure 21 : Recommended PCB Layout

8.2. BOARD TO BOARD MOUNTING

The module features a 10 pins double row 0.8mm pitch male connector from SAMTEC (FTE-105-01-G-DV-A). The host board should feature the following recommended female connector SAMTEC CLE-105-01-G-DV.

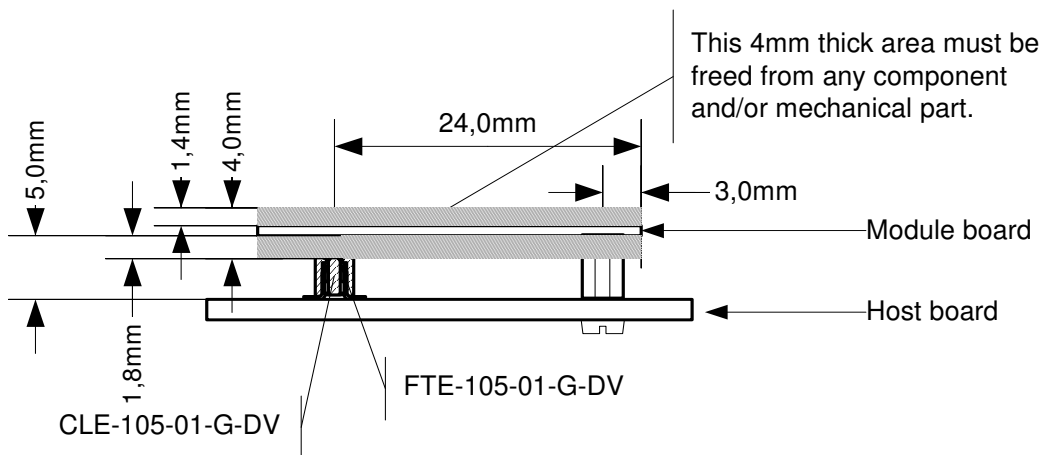


Figure 22 : Board to board mounting

From high density integration, the height of the components under the module is 1,8mm maximum (with the exception of the FTE connector). As the stacking height between the module board and the host board is 5mm high, the host board can have up to 3mm high components placed under the module.

The above figure shows an example of module fixing on a host board. The module board is tight to the host board using two M2 x 5 metallic spacers (SKIFFY PN 301 1050 400 50) and four standard screws M2 x 3. To achieve the best performance of ESD protections and EMI/RFI shielding, designer should take care to provide, on the host board, a fast electrical path to ground using only metallic spacers.

8.3. PACKAGE MECHANICAL DATA

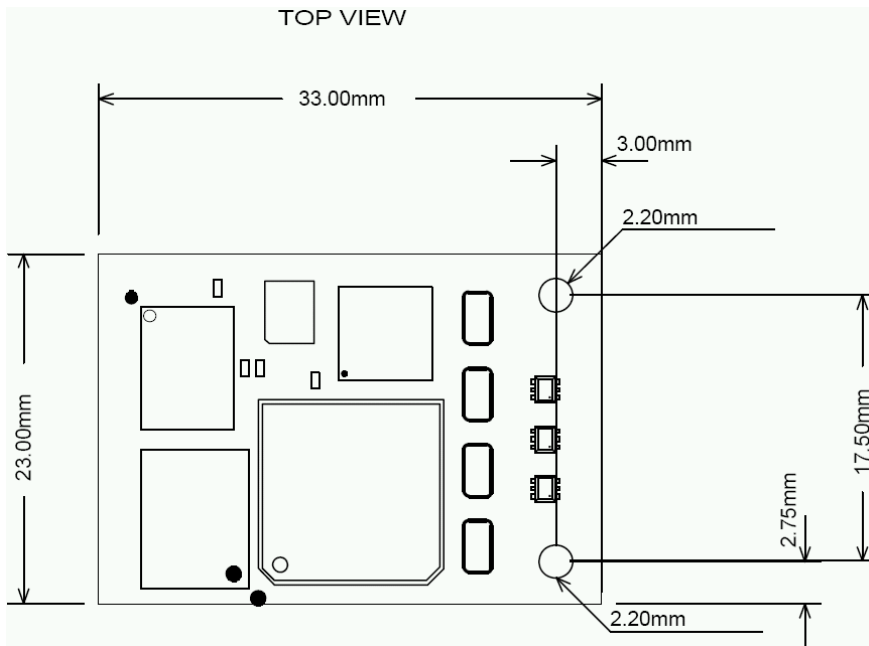


Figure 23 : Package mechanical data (Top View)

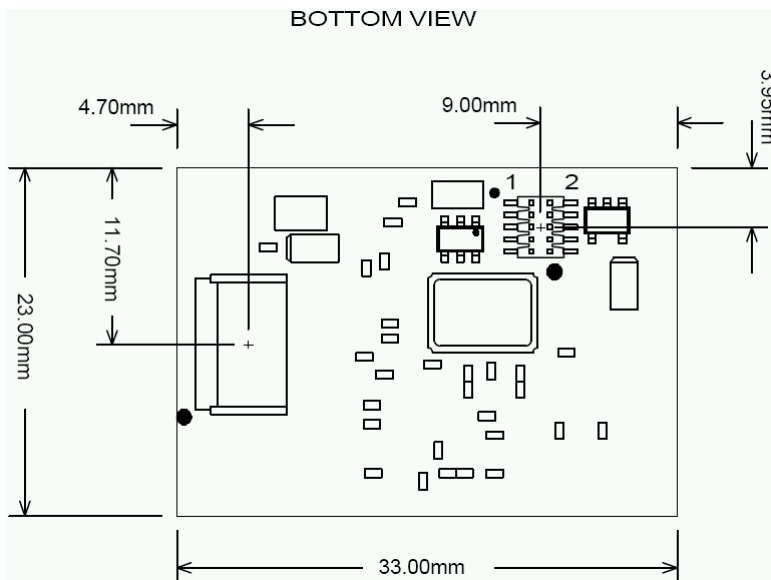


Figure 24 : Package mechanical data (Bottom View)

Dimension	Millimeters
Module width	23 mm
Module length	33 mm

9. Evaluation and Development Kit

9.1. OVERVIEW

Evaluation Kit Content

This kit is designed to evaluate the id3 "Match-On-Smartcard" technology. It includes :

- 1 BioModule MOS Evaluation Board with an integrated biometric module
- 2 smartcard readers
- 5 biometric smart cards
- 1 biometric SAM (Administrator card)
- Enrollment software for Windows 2000, XP

Development Kit Content

The BioModule Embedded Development Kit is designed to minimize development time and costs. It is used to ease the integration of the id3 and Oberthur Card System "Match-On-Smartcard" technology into an embedded target.

The software package contains not only all source files for an embedded target but also a sample application for Windows that provides great help to embedded biometric functionalities.

This kit includes :

- 1 BioModule MOS Evaluation Board with an integrated biometric module
- 1 additional BioModule MOS
- 2 smartcard readers (contact or contactless)
- 5 biometric smart cards
- 1 biometric SAM (Administrator card in ISO7810 form factor)
- Enrollment software for Windows 2000, XP
- Complete documentation, source codes and examples

9.2. BIOMODULE MOS EVALUATION BOARD

Using a BioModule Evaluation Board, the integrator can immediately run the sample application to make a fingerprint verification on a smart card.

Features

- USB bus powered
- Driver for Windows 2000, XP (The board is seen as a virtual COM port)
- Ergonomical FingerChip case designed for optimal fingerprint acquisition
- All BioModule MOS signals available on test port.

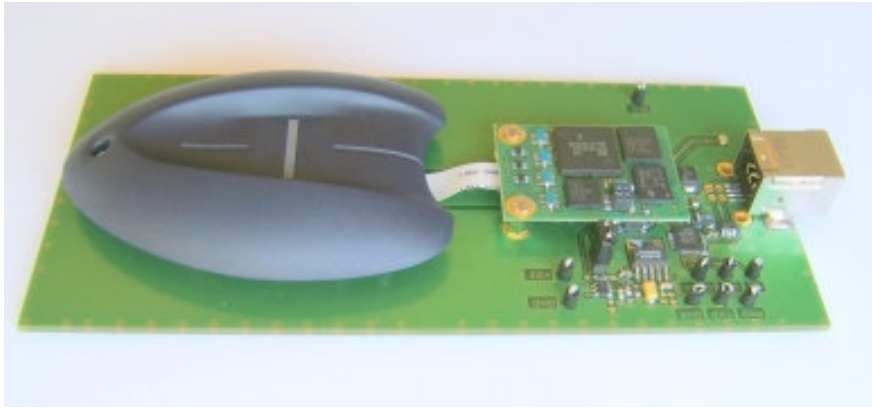


Figure 26 : BioModule Evaluation Board

9.3. APPLICATION PROGRAMMING INTERFACE

9.3.1. Communication Protocol

The BioModule provides a proprietary communication protocol (ID3NET) for easy interface with most host systems.

ID3NET protocol stack is organized in software modules for which are provided a header file (.h) and a source file (.c). Source code is written to comply with strict ANSI C and is organized using an object oriented approach.

Please refer to [2] "XSPC5K188 – BioModule Communication Protocol Software Stack Reference Guide" for detailed information.

9.3.2. BioModule API

The following table shows a summary of this API. Please refer to [3] "XSPC5K291 – BioModule Embedded Development Kit Documentation" for detailed information.

Function	Description
id3BM_ChangeImagePars	Changes the fingerprint acquisition parameters set.
id3BM_GenerateTemplate	Generates a fingerprint template from a live fingerprint.
id3BM_GetFirmwareVersion	Returns the version of the firmware.
id3BM_GetImagePars	Returns the fingerprint acquisition parameters set.
id3BM_GetProductInfo	Returns information about the product.
id3BM_GetTemplate	Returns the fingerprint template previously generated.
id3BM_SaveParameters	Saves current module parameters into persistent storage area

9.3.3. Biometric Smart Card API

The following table shows a summary of this API. Please refer to [3] "XSPC5K291 – BioModule Embedded Development Kit Documentation" for detailed information.

Function	Description
id3BSC_CloseSecureChannel	Closes a secure channel previously established between a smart card and a SAM.
id3BSC_DeleteFingerprint	Deletes an existing fingerprint template from a smart card.
id3BSC_EnrollFingerprint	Enrolls a fingerprint template on a smart card.
id3BSC_InitCryptoSystem	Initializes the biometric crypto-system on the smart card (or SAM).

id3BSC_OpenSecureChannel	Establishes a secure channel between the smart card and the SAM.
id3BSC_SelectApplication	Selects the AuthentIC-BIO Application on the smart card.
id3BSC_Transmit	Sends a service request to the smart card, and expects to receive data back from the smart card.
id3BSC_VerifyFingerprint	Performs a fingerprint template verification on a smart card.

9.3.4. Documentation Support

For software integration, please consult the following documentation:

- XSPC5J080 – BioModule Command Specifications
- XSPC5K188 – BioModule Communication Protocol Software Stack Reference Guide
- XSPC5K291 – BioModule Embedded Development Kit Documentation

9.4. AUTHENTIC BIOMETRY KIT

The AuthentIC Biometry JDK (JavaCard Development Kit) is provided as a developer companion of the CosmopolIC v5 smartcard. It comprises the following elements:

- A JavaCard package that allows a programmer to take benefit of the AuthentIC Biometry solution in his own applets,
- The requirements, in term of supported APDU commands, for an applet to comply with the BioModule MOS and the BioModule EDK,
- Full code of applets implementing biometric verification and guidelines regarding the host application that communicates with these applets via the BioModule EDK.

10. Ordering Information

10.1. REFERENCES

Item	Reference
Fingerprint Recognition Module	085E4170
Fingerprint Recognition Module with 50mm flex cable and AT77C101B-CB01 sensor	085K3340
50mm long 0,3mm pitch flex cable	182E1500
BioModule Evaluation Board	085D4610
BioModule MOS Evaluation Kit	086N2990
BioModule MOS Development Kit	086N3000

Table 10 : Ordering Information

For any further information, please contact contact@id3semiconductors.com.

10.2. CONTACT US



id3 Semiconductors
5, rue de la Verrerie
F 38120 Le Fontanil Cornillon
FRANCE

T : (+33) 04 76 75 75 85

F : (+33) 04 76 75 52 30

Home page : <http://www.id3semiconductors.com>

Contact : contact@id3semiconductors.com