eFM500F

Powered by MS500

DATASHEET

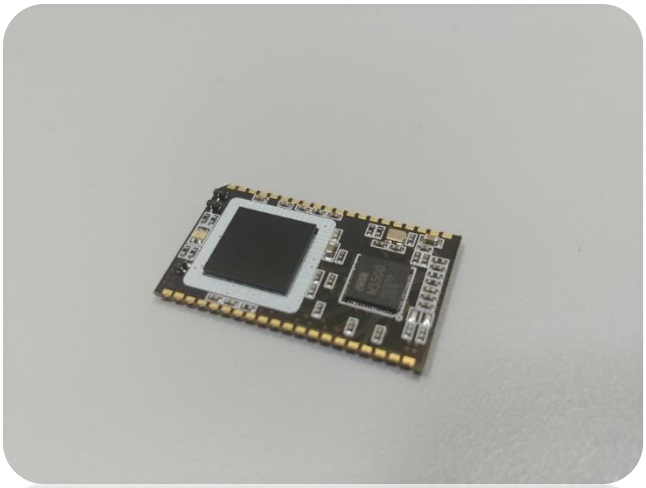
Ver 0.3

DOCUMENT REVISION AND REFERENCE

Revision History

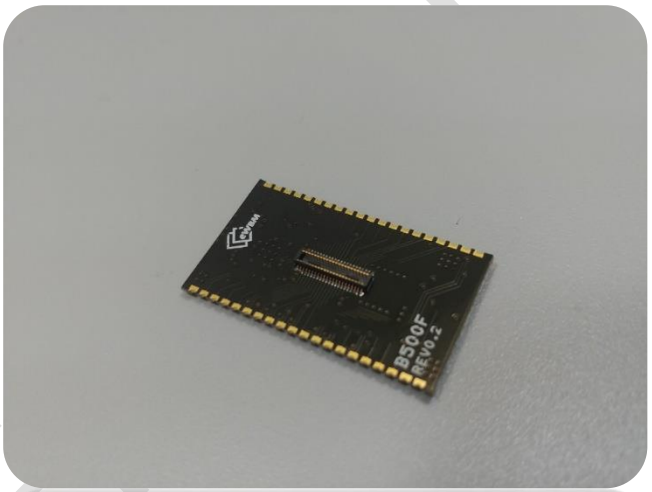
Revision	Date	Description
0.1	02-Oct-2018	1st Release
0.2	17-Oct-2018	Add Command
0.3	18-Oct-2018	Modify Command Terminology

FEATURES



Top View

Bottom View



The eFM500 is a secure fingerprint module for a fingerprint recognition application of a system device with high security features.
This module stores fingerprint metadata, which was generated by module's software from scanned image, encrypted using internally hidden cryptography key, and therefore the metadata template cannot be taken out by any mean.

The eFM500 consists of a fingerprint sensor which is spoofing free compared to general fingerprint scanner and MS500, a secure MCU, for fingerprint processing including fingerprint template generation to be securely stored and matching the new capture with the reference templates.

The eFM500 is available in two form factors: "eFM500F" is a full version with rich interfaces and "eFM500S" with smaller number of interfaces.

MCU [MS500] Features

CPU Core

- Core: ARM Cortex-M0 @100MHz

Memory and Interface

- Internal Flash Memory: 4 MB in MS500
- Interface: SDMMC Ver 3.01 1-Ch, UART 2-Ch, I2C 1-Ch, SPI-1Ch, GPIO Max. 24 Port

Security Features

- Secure Key Management
  - Device Unique Key
  - Platform Key
  - User Defined Key
  - Session/App Key
- Secure Boot – Firmware Integrity Checking
- Secure Storage

Hardware Crypto Engines

- Symmetric Crypto engines
  - AES 128/192/256 strength
  - ARIA 128/192/256 for Korean market
- Asymmetric Crypto engines
  - ECC up to 512 strength
  - RSA up to 2048 strength
- Hash Accelerator – SHA1/SHA256 (50MB/sec)
- TRNG – Ture Random Number Generator (25Mbps)
- HMAC (Hash-based MAC)
- Authentication Algorithms
  - AES GCM/GMAC
  - AES CCM/CBC-MAC
- AES Encryption Mode: ECB, CBC, CTR

Fingerprint Sensor Features

- Fingerprint area sensor with capacitive sensing method
- Pixel Resolution: 508dpi (50um x 50um)
- Sensing Array: 160C x 160R
- Sensing Area: 8,000um x 8,000um
- Mode0 SPI up to 12MHz and one IRQ signal for Host Interface
- 8bit ADC with 256 gray scale
- Finger Detection/Click, Flexible size image capture, image read accelerating

TABLE OF CONTENTS

1 . INTRODUCTION

1.1 OVERVIEW

The eFM500F is a stand-alone, fingerprint recognition module that lets a user easily register, store, and delete fingerprint information. Not only can the user use a simple hardware board-to-board connection, but the user can also add a fingerprint recognition feature more easily.

The eFM500F consists of MS500, a secure MCU, and a 160x160 arrayed fingerprint sensor. Users can register three (3) separate fingerprints into this module. In addition, the fingerprint metadata acquired from the eFM500F module is encrypted by the MS500's hardware crypto engine and stored in its secure memory area. This mechanism protects the module from any potential hacking threat.

In the event that the device with this module may be lost or broken, it is not possible to fetch the fingerprint metadata.

1.2 BLOCK DIAGRAM

An architectural overview of the eFM500F Diagram is as below:

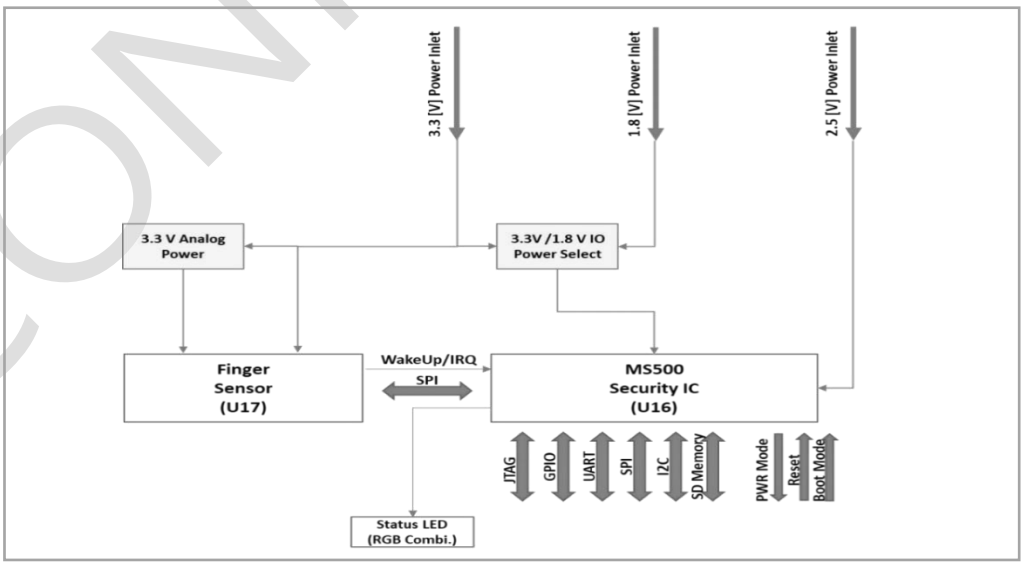


Figure 1-1. B500F Block Diagram

2 . SECURE MCU [MS500] of eFM500F

2.1 SECURE MCU [MS500]

The secure MCU [MS500] of eFM500F is based on the ARM Cortex-M0 32-bit CPU core. It is RISC microcontroller with Hardware Security Block for embedded applications featuring a high level of integration and low-power consumption

ARM Cortex-M0 Processor

The ARM Cortex-M0 incorporates a 3-stage pipeline von Neumann architecture with separate buses for instruction cache, data sync-up cache, and cache of shadow remap, making it ideal for demanding embedded application. The Cortex-M0 processor also implements the ARMv6-M architecture, which is based on the 16-bit Thumb instruction set that provides the exceptional performance expected of a modern 32-bit architecture, with a higher code density than other 8-bit and 16-bit microcontrollers. In addition, Cortex-M0 closely integrates a configurable Nested Vectored Interrupt Controller (NVIC), to deliver industry-leading interrupt performance

Nested Vectored Interrupt Controller (NVIC)

The NVIC and the processor core interface are tightly coupled to enable low interrupt latency and efficient processing of late arriving interrupts. It includes 32 interrupt inputs and a Wakeup Interrupt Controller (WIC) When the main processor is in Deep Sleep mode the WIC can wake up the processor. This allows the power to be switched off to the main processor when it is not in use.

BOOT ROM

The MS500 MCU of eFM500F contains internal ROM memory which is used to store the boot code for the ARM Cortex-M0. When the ARM Cortex-M0 processor is released from reset, it immediately starts to execute the boot code stored in this ROM. The size of ROM is 8 KB at peak

Flash Memory

Flash memory used to permanently store device/system configuration settings, software-specific configuration information and user-defined information. The size of flash memory in MS500 is 4 MB.

Non-Volatile Memory (NVM)

The eFuse memory is a non-volatile, one-time programmable memory used to permanently store device/system configuration settings, software-specific configuration information and user-defined information.

The eFuse memory also contains device specific information including device ID (DID), platform key (PFK), device unique key (DUK), and a user definable key. For details on how to program eFuse with customer specific information, please contact eWBM's technical support.

A 1024-bits high-density electrical Fuse can be programmed by eWBM for Customer with special condition.

2.2 USER INTERFACES

SPI

The MS500's SPI master/slave interfaces can communicate up to a speed of 50 Mbit/s in either full-duplex or half-duplex communication modes. During a data transfer, the master always sends 4~16bits of data to the slave, and the slave always sends 4~16 bits of data to the master.

Note 1: This speed is measured with Raspberry Pi3 Model board in typical test environments. That speed is somewhat influenced by whether the board state and temperature environments.

The MS500's SPI Interface includes the following features:

- Maximum data bit rate of one eighth of the APB clock (PCLK) rate
- Support three chip-selects output, serial-master and serial-slave mode, and software configurable.
- Master mode baud rate prescaler
- DMA-based or interrupt-based operation.
- Master and slave operation.
- 8x16 FIFOs for transmit and receive.
- Provide programmable loop-back mode for self-test operation.
- Interact with multiple masters and slaves on the bus.
- Separate Serial Clock from APB clock

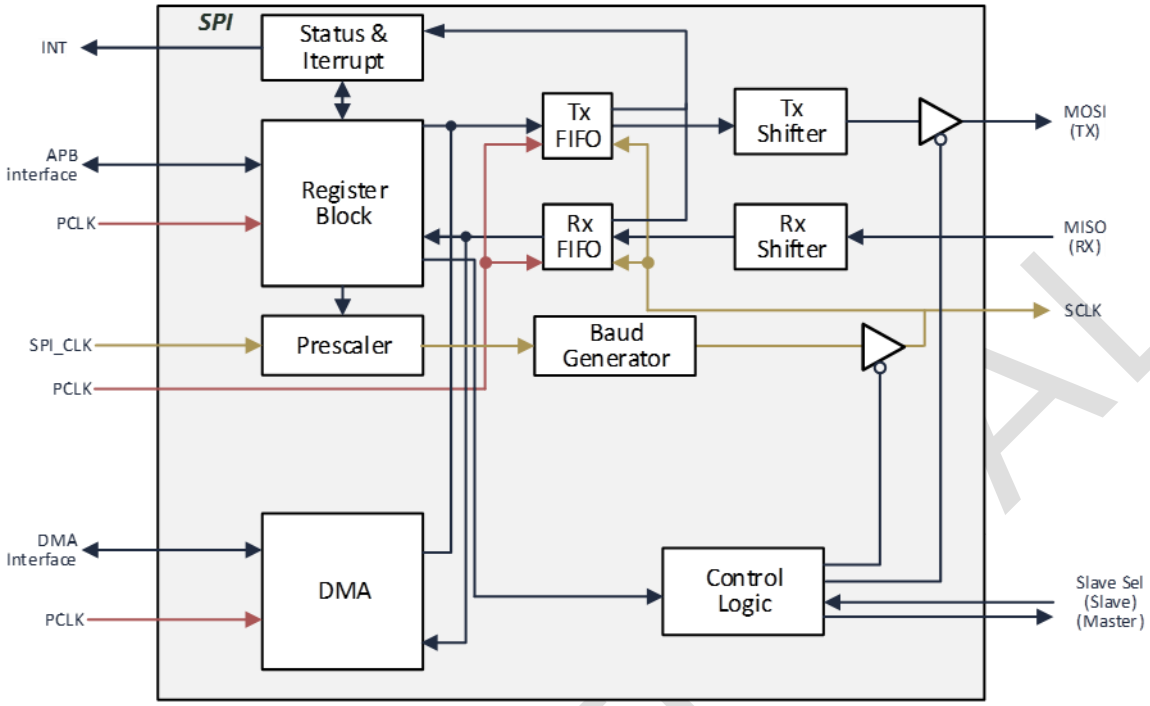


Figure 2-1. SPI Block Diagram

UART

The UARTs include the following features:

- Data sizes of 5, 6, 7, and 8 bits.
- Register locations conform to industry-standard 16C550.
- 1, 1.5, or 2 stop bit generation.
- Parity generation and detection; even, odd, stick or no-parity bit.
- Line break generation and detection.
- Programmable baud rate generator. This enables division of the reference clock by (1x16) to (65535 x16) and generates an internal x16 clock. The divisor can be a fractional number enabling you to use any clock with a frequency >3.6864MHz as the reference clock.
- Provide programmable loop-back mode for self-test operation.
- Separate 16x8 transit and 16x11 receive FIFOs to reduce CPU interrupt.
- Support for DMA.
- Support of the modem control functions CTS, DCD, DSR, RTS, DTR, and RI.

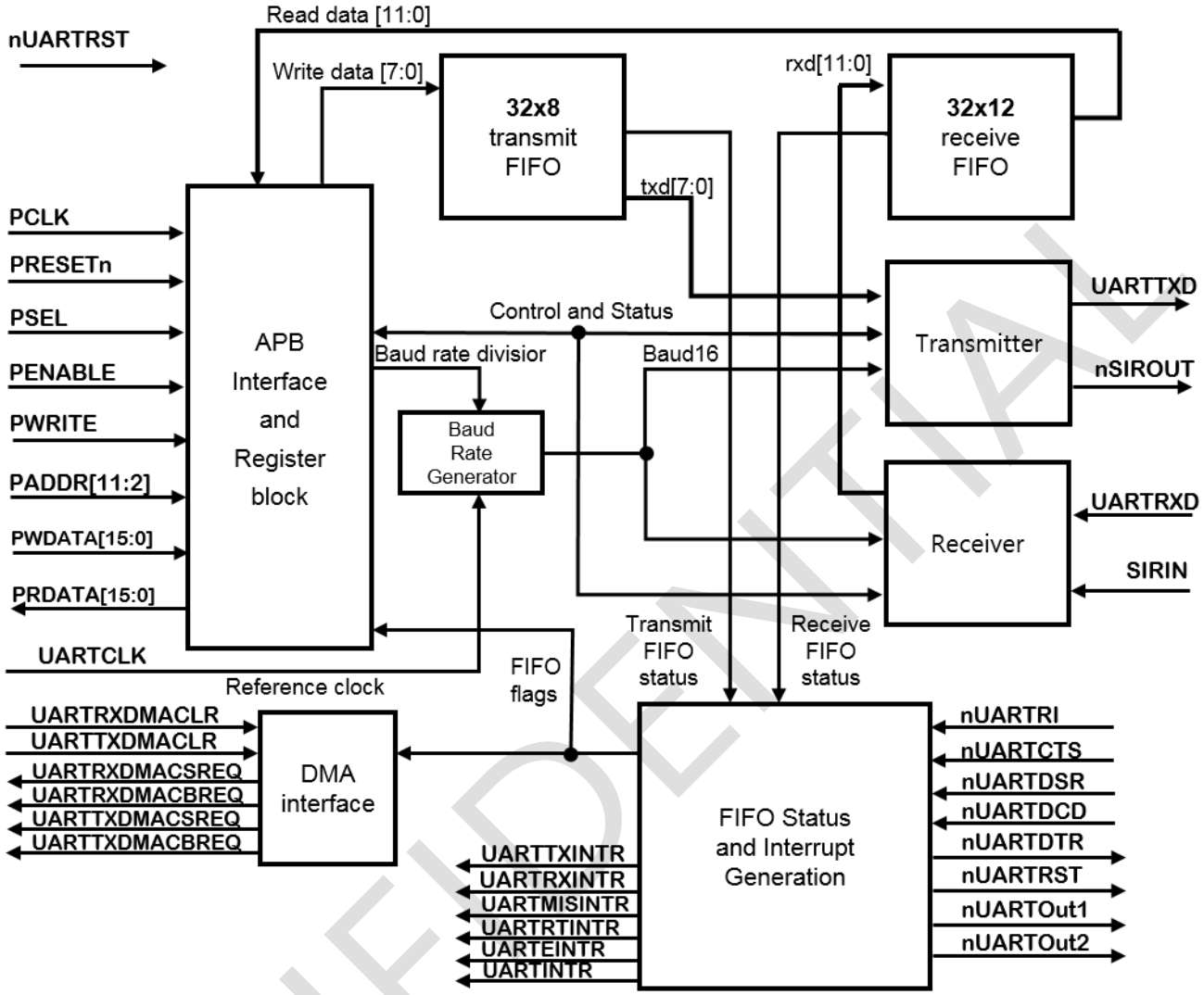


Figure 2-2. UART Block Diagram

I2C

The I²C-bus is bidirectional interface for inter-IC control communication using only two wires: a Serial Clock line (SCL) and a Serial Data line (SDA). Each device is recognized by a unique address and can operate as either a receiver-only device or as a transmitter with the capability to both receive and send information.

Transmitters and/or receivers can operate in either master or slave mode, depending on whether the device is initiating data transfer or if it is only being addressed. The I²C is a multi-master bus and can be controlled by more than one bus master connected to it.

The MS500's I²C interface consists of the following features:

- Standard I²C-compliant bus interfaces may be configured as a Master or a Slave
- Supports both transmitting and receiving data as a master or a slave
- Supports simultaneous master and slave operation
- Arbitration is handled between simultaneously transmitting masters without corruption of serial data on the bus.
- Programmable clock allows adjustment of I²C transfer rates.
- Data transfer is bidirectional between masters and slaves.
- Serial clock synchronization allows devices with different bit rates to communicate via one serial bus.
- Serial clock synchronization is used as a handshake mechanism to suspend and resume serial transfer.
- Supports Fast-mode Plus with data rates of up to 400kbit/s.
- Optional recognition of up to four distinct slave addresses.
- Monitor mode allows observing all I²C-bus traffic, regardless of slave address.
- I²C-bus can be used for test and diagnostic purposes.
- The I²C-bus contains a standard I²C-compliant bus interface with two pins

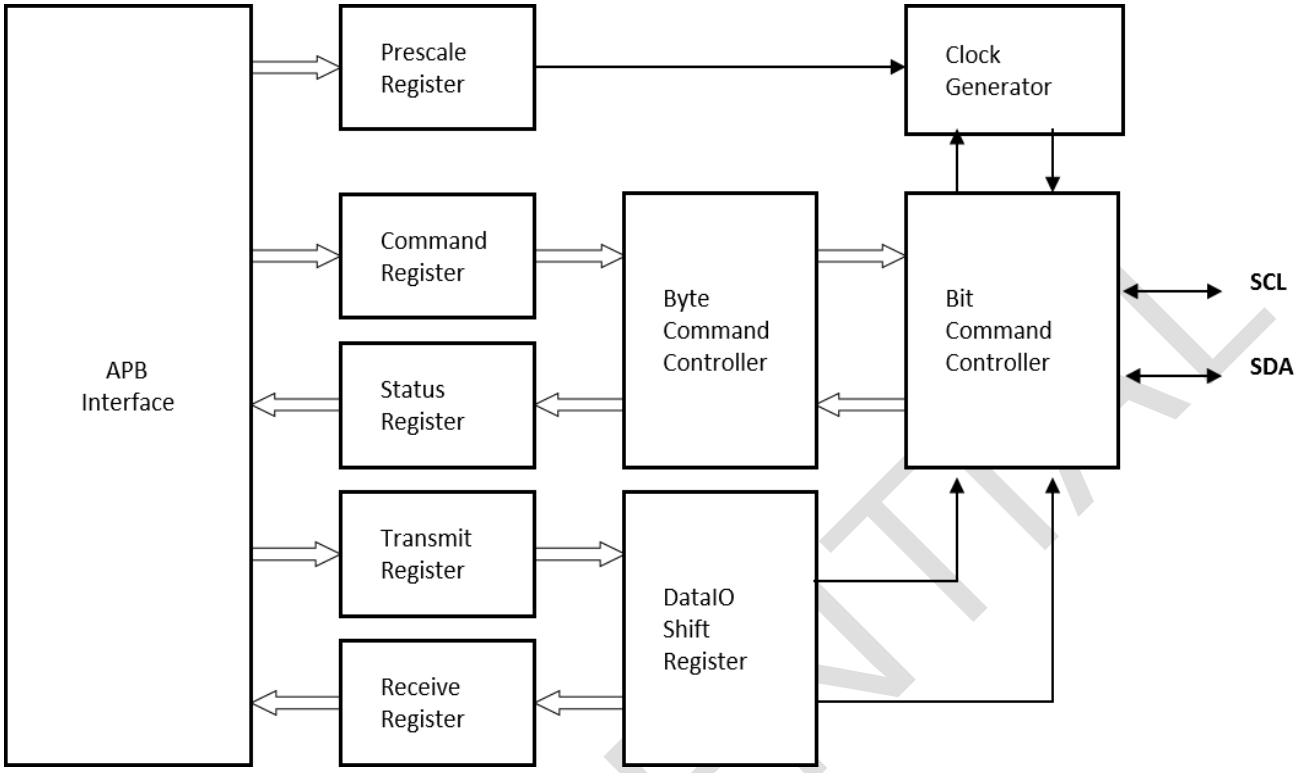


Figure 2-3. I²C Block Diagram

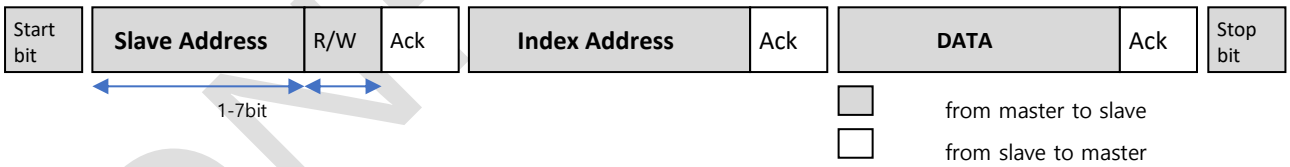


Figure 2-4. I2C Data Transfer

The external I²C mater should send to MS500's I²C slave as below procedure

- Method of transmitting data to an I²C slave from an I²C master shall proceed in the following order.
- The master sends the slave address and waits for an ACK from the slave.
- After receiving the ACK, the master will send a 1byte of index address and wait for an ACK from the slave. This index address can be set to a temporary value.
- After receiving the ACK, the master will send a 1byte of data and wait for an ACK from the slave

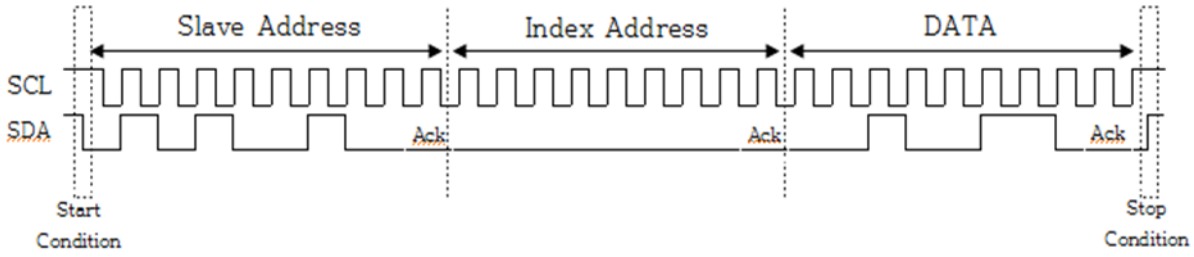


Figure 2-5. Typical I2C Master Transfer

GENERAL PURPOSE I/O (GPIO)

The GPIO pins can be used in several ways to set pins as inputs or outputs and use the inputs as combinations of level and edge sensitive interrupts

GPIO Pin Interrupt Features

- all GPIO support edge- or level-sensitive interrupt request. Each request creates a separate interrupt in the NVIC.
- It supports fast toggle changes.
- Edge-sensitive interrupt pins can interrupt on rising or falling edges or both.
- Level-sensitive interrupt pins can be configured as active HIGH or LOW active.
- Separated bus interface and free running clocks to support CPU sleep.

GPIO Group interrupt features

- The inputs from any number of GPIO pins can be enabled to contribute to a combined group interrupt.
- The polarity of each input enabled for the group interrupt can be configured HIGH or LOW.
- Enabled interrupts can be logically combined through an OR/AND operation.
- Two group interrupts are supported to reflect two distinct interrupt patterns.
- The GPIO group interrupts can wake up from sleep/deep sleep modes.

GPIO Port Features

- GPIO pins can be configured as input or output by software.
- All GPIO pins default to inputs with interrupt disabled at reset.
- Pin registers allow pins to be sensed and set individually.

2.3 SECURITY BLOCK

The Security Block consists of the ACA, SCA and TRNG.

ACA (Asymmetrical Crypto Accelerator)

The ACA is designed to offload large arithmetic operations from the host CPU. The host only needs to load the parameters in the ACA and specify the appropriate function to initiate the autonomous program.

No further communication between the ACA and the system is required until the ACA finishes performing the requested operation.

The large arithmetic operations performed by the ACA provide acceleration of the following PKI operations.

- RSA (with or without CRT): 512, 768, 1024, 1536, 2048-bit
- ECC-GF(p): 160, 192, 224, 256, 384, 512-bit

SCA (Symmetric Crypto Accelerator)

SCA performs parallel hashing and encryption/decryption operations with hardwired acceleration engine. The SCA provides a framework including a programmable sequencer, DMA engine, and cryptographic/hashing resources that may handle a variety of protocols involving a cipher and a hash. The SCA also optimizes cryptographic offload for bulk processing of cipher and hash algorithms, as well as combined mode algorithms (e.g. GCM, CCM).

- The features supported by SCA are listed below:
- Cipher algorithms: AES
- Cipher modes: ECB, CBC, CTR, CCM, GCM
- Hash (MAC) algorithms: SHA-1, SHA-256
- Hash modes: Raw HMAC.

- independent cryptographic contexts
- FIFO based command/status interface which allows queuing of multiple packets by the host CPU
- Full DMA master which uses data descriptor tables to automatically read and write fragmented data packets to be processed. Packet data traverses the bus only twice per packet (once for the read operation, once for the write operation)
- Secure key port for block cipher algorithms (AES).

ARIA

The ARIA (Academy, Research Institute, Agency) module is Korean cryptographic algorithm for public use and support 128/192/256bit key length and encrypt/decrypt input data with key value

- ARIA Hardwire Engine with key length 128, 192, 256-bit
- Can Operate with DMA engine to high speed operation
- Highly optimized hardware engine without internal memory

TRNG

TRNG (True Random Number Generator) generates random data that is statically equivalent to a uniformly distributed random data stream.

- Continuous random bit stream generation
- Automatic seed/reseed from internal random noise source
- Manual seed/reseed by host CPU
- HIGH Speed 25Mbps at 100MHz

3 . PIN ASIGNMENT

The power and signal assignment of the eFM500F module are shown below.

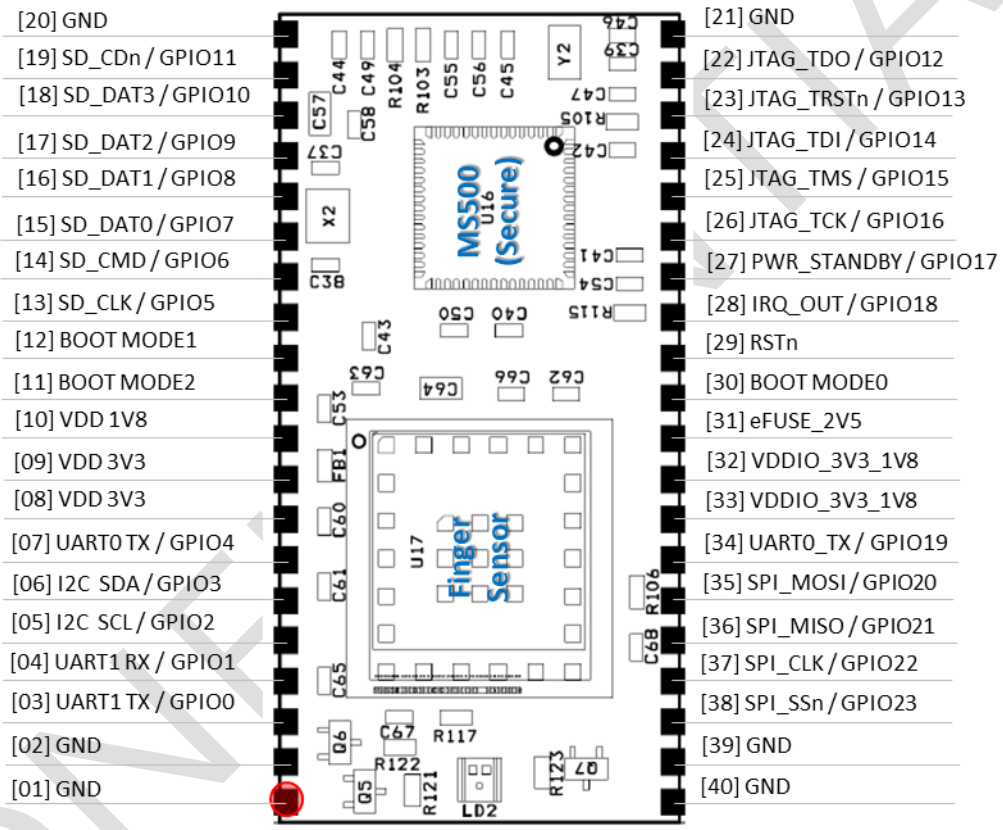


Figure 3-1. eFM500F Module's Signal Asign

4 . OPERATION

The eFM500F enables the Progress of Fingerprint Recognition, Registration and Deletion inside the Module.

4.1 OPERATION MODE

The modes of operation include Verification, Deletion, Enrollment and User Authentication.

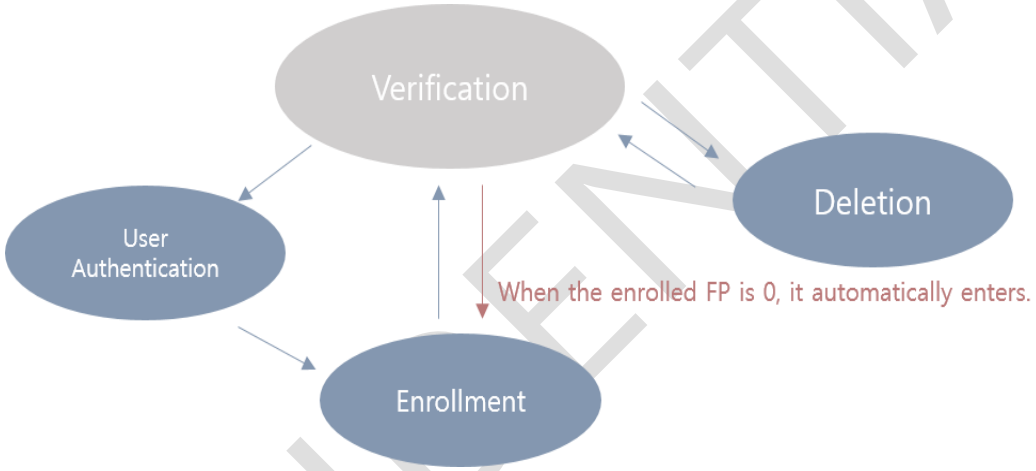


Figure 4-1 Operation Mode

Verification

Verification is the basic mode of eFM500F. It compares the detected fingerprint with the stored fingerprint template generated by the enrollment process and confirms whether it matches. The result of the match can be checked by the color change of the LED mounted on the module. When the external device is interlocked, it can receive the matching result using the communication protocol supported by the eFM500F module.

User Authentication

This is a mode in which a registered user confirms a new registration to prevent irrelevant fingerprint registration. After the confirming already registered user, module enters the enrollment mode for the fingerprint registration.

Enrollment

This is a mode for registering a new fingerprint. Touch the sensor pad lightly with the finger five (5) times following the LED color indication messages. This sensor uses the capacitive scanner to provide the fingerprint data. The Scanning Fingerprint position shall be slightly different for each entry to cover most of the fingerprint area.

Deletion

This is a mode to delete the registered fingerprint template. Before deleting an existing template, the user must check the fingerprint and scan the fingerprint again for the deletion. If the detected fingerprint does not match the template, the deletion procedure will not proceed.

[Table 4-1] The Operation Mode of eFM500F

Mode	Enter	Exit
Verification	After the Booting	
User Authentication	When the finger touches the sensor 3 times in the verification mode	When the detected fingerprint on the sensor matches that of the registered users on the template When the same fingerprint is detected 3 times continuously (Forced Exit) When no fingerprint is detected for 30 seconds (Forced Exit: TBD)
Enrollment	Already registered user gets confirmed In the User Authentication mode Automatic entry if there is no registered fingerprint after the booting	When the fingerprint is registered completely When the same fingerprint is detected 3 times continuously (Forced Exit) When fingerprint is not detected for 30 seconds (Forced Exit: TBD)

Deletion	When the duplicate fingerprint is detected	When the fingerprint is removed completely When the duplicate fingerprint is detected (Forced Exit) When fingerprint is not detected for 30 seconds (Forced Exit: TBD)

4.2 LED INDICATOR

[Table 4-2] The Meaning of LED Indicator

Mode	Meaning	Indication
Verification	Waiting	LED off
	Recognition Success	Green 3 seconds lighting
	Recognition Failure	Red lights solid
User Authentication	Waiting	Blue flashing
	Recognition Success	Green 3 seconds lighting
	Recognition Failure	Red lights solid
Enrollment	Waiting	Blue lights solid
	Recognition Success	Green lights solid
	Recognition Failure	Red lights solid
	Registration Complete	Purple 3 seconds lighting
Deletion	Waiting	White lights solid
	Recognition Failure	Red lights solid
	Delete Complete	Green 3 seconds lighting

5 . COMMAND

In this section, the commands checking the operation status and controlling the fingerprint module are described.

eFM500F's commands can be roughly divided into three categories as follows: an interrupt command, a response command, a request command.

Interrupt Command (eFM500F → Host)

This is a command initiated by the eFM500F module. The command informs the host of eFM500F module

with the enrollment entry/result, and the verification entry/result as well as the error status.

[Table 5-1] Interrupt Command Description

Name	Description	Command
INT_OP_MODE	Informs the operation mode status, either the verification mode or the enrollment mode	0x01
INT_ENROLL	Informs when the fingerprint is registered in the enrollment mode	0x02
INT_VERIFY	Informs when the fingerprint is recognized in the verification mode	0x03
INT_ERROR	Informs when an error occurred in the verification mode or the enrollment mode	0x04
INT_DELETE	Informs the deletion mode	0x05

- ✓ Verify: Fingerprint recognition mode
- ✓ Enroll: Fingerprint enroll mode

Response Command (eFM500F → Host)

This is a command caused by the eFM500F module. The command prompts with the response to the host request command.

[Table 5-2] Response Command Description

Name	Description	Command
RSP_GET_OP_MODE	Prompts with the current operation mode	0x10
RSP_GET_ENROLLED_FP	Prompts with the number of registered fingerprints request	0x11
RSP_SET_LED_CTRL_HOST	Prompts with the LED control host setting	0x12
RSP_SET_OP_MODE	Prompts with the running mode setting. **[TBD]**	0x13
RSP_SET_CTRL_HOST	Prompts with the control host setting. **[TBD]**	0x14
RSP_GET_VERSION	Prompts with the version number request	0x15
RSP_SET_LED_COLOR	Prompts with the LED color setting	0x16
RSP_SET_ENROLL_EXIT	Prompts with exit Enrollment [**TBD]**	0x17

Request Command (User's System → eFM500F)

This is a command caused by user's system. The command prompts when the information such as operation mode, control mode and version of eFM500F is requested.

[Table 5-3] Request Command Description

Command	Description	Command
REQ_GET_OP_MODE	Prompt for the current operation mode	0x20
REQ_GET_ENROLLED_FP	Prompt for the number of registered fingerprints	0x21
REQ_SET_LED_CTRL_HOST	Prompt for the LED control host setting	0x22
REQ_SET_OP_MODE	Prompt for the operation mode setting **[TBD]**	0x23
REQ_SET_CTRL_HOST	Prompt for the control host setting. **[TBD]**	0x24
REQ_GET_VERSION	Prompt for the version number	0x25
REQ_SET_LED_COLOR	Prompt for the LED color setting (It's available when LED control host is slave only) **[TBD]**	0x26
REQ_SET_ENROLL_EXIT	Prompt to exit Enrollment setting **[TBD]**	0x27

5.1 INTERRUPT COMMAND

INT_OP_MODE

- This command indicates the verification mode status or the enrollment mode status.

[Table 5-4] INT_OP_MODE

CMD	DAT0	DAT1	DAT2	DAT3
0x01	Reserved			Run Mode

- **[DAT3]** Run Mode
- 0x00 : Verification Mode
- 0x01 : Enrollment Mode
- 0x02 : Deletion Mode
- 0x03 : Pre-Enrollment Mode (To prevent the enrollment of unauthenticated user's fingerprints, the enrollment is authenticated by already enrolled user, before the enrollment mode,)

INT_ENROLL

- The command indicates that the detected fingerprint is in the enrollment mode

[Table 5-5] INT_ENROLL

CMD	DAT0	DAT1	DAT2	DAT3
0x02	Reserved		Count	Result

- **[DAT2]** Count
  - ✓ 0xXX : Fingerprint Recognition Count (Max 5)
- **[DAT3]** Result
  - ✓ 0x00 : Invalid Fingerprint
  - ✓ 0x01 : Fingerprint Enrollment Processing
  - ✓ 0x02 : Fingerprint Enrollment Success

INT_VERIFY

- The command indicates the verification mode Status.

[Table 5-6] INT_VERIFY

CMD	DAT0	DAT1	DAT2	DAT3
0x03	Reserved			Result

- **[DAT3]** Result
  - ✓ 0x00 : Invalid Fingerprint
  - ✓ 0x01 : Fingerprint Recognition Success

INT_ERROR

- The command indicates the error in the verification mode or in the enrollment mode

[Table 5-7] INT_ERROR

CMD	DAT0	DAT1	DAT2	DAT3
0x04	Reserved			Error

- **[DAT3]** Error
  - ✓ 0x00 : No more fingerprints can be registered
  - ✓ 0x01 : No Registered fingerprints
  - ✓ 0x02 : Does not match registered fingerprint **(TBD)**
  - ✓ 0x03 : Sensor no response **(TBD)**
  - ✓ 0x04 : Unable to delete fingerprint **(TBD)**

INT_DELETE

- The command indicates the deletion mode Status

[Table 5-8] INT_DELETE

CMD	DAT0	DAT1	DAT2	DAT3
0x05	Reserved			Result

- **[DAT3]** Result
  - ✓ 0x00 : Invalid Fingerprint
  - ✓ 0x01 : Waiting for Fingerprint Deletion **(TBD)**
  - ✓ 0x02 : Fingerprint Deletion Success

5.2 RESPONSE COMMAND

RSP_GET_OP_MODE

- The command provides the current operation mode request.

[Table 5-9] RSP_GET_OP_MODE

CMD	DAT0	DAT1	DAT2	DAT3
0x10	Reserved			Mode

- **[DAT3]** Mode
  - ✓ 0x00 : Verification Mode
  - ✓ 0x01 : Enrollment Mode
  - ✓ 0x02 : Deletion Mode
  - ✓ 0x03 : Pre-Enrollment Mode

RSP_GET_ENROLLED_FP

- The command provides the number of registered fingerprints request (Max. 3)

[Table 5-10] RSP_GET_ENROLLED_FP

CMD	DAT0	DAT1	DAT2	DAT3
0x11	Reserved			Enrolled FP

- **[DAT3]** Enrolled FP
  - ✓ 0xXX : Number of Fingerprints Registered on the Device (Max 3)

RSP_SET_LED_CTRL_HOST

- The command provides the LED control host setting.

[Table 5-11] RSP_SET_LED_CTRL_MODE

CMD	DAT0	DAT1	DAT2	DAT3
0x12	Reserved			Result

- **[DAT3]** Result
  - ✓ 0x00 : Slave (Control by User's system)
  - ✓ 0x01 : Master (LED controlled by eFM500F automatically – Default)

RSP_SET_OP_MODE (TBD)

- The command provides the running mode setting.

[Table 5-12] RSP_SET_OP_MODE

CMD	DAT0	DAT1	DAT2	DAT3
0x13	Reserved			Result

RSP_SET_CTRL_HOST (TBD)

- The command provides the control host setting

[Table 5-13] RSP_SET_CTRL_HOST

CMD	DAT0	DAT1	DAT2	DAT3
0x14	Reserved			Result

- **[DAT3]** Result
  - ✓ 0x00 : Slave (User's system control operation mode)
  - ✓ 0x01 : Master (eFM500F control operation mode – Default)

RSP_GET_VERSION

- The command provides the version number request

  (The version is "X.XX" type, the left part of the point is High Ver, and the Right part is Low Ver.)

[Table 5-14] RSP_GET_VERSION

CMD	DAT0	DAT1	DAT2	DAT3
0x15	Reserved		High Ver	Low Ver

- **[DAT2]** High Ver
  - ✓ 0xXX : High Version
- **[DAT3]** Low Ver
  - ✓ 0xXX : Low Version

RSP_SET_LED_COLOR

- The command provides the LED color setting

[Table 5-15] RST_SET_LED_COLOR

CMD	DAT0	DAT1	DAT2	DAT3
0x16	Reserved	Red	Green	Blue

- [DAT1] Red / [DAT2] Green / [DAT3] Blue
  - ✓ 0x00 : Off
  - ✓ 0x01 : On
  - ✓ 0x02 : FAIL (LED_CTRL_HOST is Master(eFM500F Module)

5.3 REQUEST COMMAND

REQ_GET_OP_MODE

- The command requests for the current operation mode

[Table 5-16] REQ_GET_OP_MODE

CMD	DAT0	DAT1	DAT2	DAT3
0x20	0x00	0x00	0x00	0x00

REQ_GET_ENROLLED_FP

- The command requests for the number of registered fingerprints

[Table 5-17] REQ_GET_ENROOLED_FP

CMD	DAT0	DAT1	DAT2	DAT3
0x21	0x00	0x00	0x00	0x00

REQ_SET_LED_CTRL_HOST

- The command requests for the LED control host setting

[Table 5-18] REQ_SET_LED_HOST

CMD	DAT0	DAT1	DAT2	DAT3
0x22	Reserved			LED Control

- LED Control
  - ✓ 0x00 : Slave (Controlled by User's system)
  - ✓ 0x01 : Master (Controlled by eFM500F automatically – Default)

REQ_SET_OP_MODE (TBD)

- The command requests for the operation mode setting

[Table 5-19] REQ_SET_OP_MODE

CMD	DAT0	DAT1	DAT2	DAT3
0x23	Reserved			Run Mode

- **[DAT3]** Run Mode
  - ✓ 0x00 : Verification Mode
  - ✓ 0x01 : Enrollment Mode
  - ✓ 0x02 : Deletion Mode
  - ✓ 0x03 : Pre-Enrollment Mode

REQ_SET_CTRL_HOST (TBD)

- The command requests for the control host setting.

[Table 5-20] REQ_SET_CTRL_HOST

CMD	DAT0	DAT1	DAT2	DAT3
0x24	Reserved			Control Master

- **[DAT3]** Control Master

  0x00 : Slave (Controlled by User's system)

  0x01 : Master (Controlled by eFM500F automatically [Default])

REQ_GET_VERSION

- The command requests for the version number.

[Table 5-21] REQ_GET_VERSION

CMD	DAT0	DAT1	DAT2	DAT3
0x25	0x00	0x00	0x00	0x00

REQ_SET_LED_COLOR

- The command requests for the LED color setting

  (It's available when LED control host is slave only)

[Table 5-22] REQ_SET_LED_COLOR

CMD	DAT0	DAT1	DAT2	DAT3
0x26	Reserved	Red	Green	Blue

- [DAT1] Red / [DAT2] Green / [DAT3] Blue
  - ✓ 0x00 : Off
  - ✓ 0x01 : On

REQ_SET_ENROLL_EXIT (TBD)

- The command requests for the enrollment exit setting.

[Table 5-23] REQ_SET_ENROLL_EXIT

CMD	DAT0	DAT1	DAT2	DAT3
0x27	0x00	0x00	0x00	0x00

6 . DATA PACKET

6.1 UART Packet

[Table 6-1] UART_Packet

STX	CMD	DAT0	DAT1	DAT2	DAT3	CS	ETX
0xFA	Interrupt or Response or Request PACKET					0xXX	0xFE

- CS = CMD^DAT0^DAT1^DAT2^DAT3+0x01
- Baud Rate = 115200bps

6.2 SPI Packet

TBD

[설명 입력]

6.3 I2C Packet

TBD

7 . ELECTRICAL SPECIFICATION

7.1 OPERATION POWER RANGE

[Table 7-1] Operation Power Table

Parameter	Symbol	Min	Typ.	Max	Units
Main Power	VCC_SYS	3.0	3.3	3.6	V
BF30A Analog Power	VDD_3V3	3.0	3.3	3.6	V
MS500 Flash Power	VDD_1V8	1.7	1.8	1.9	V
eFuse power	MS_eFUSE_EN_2V5	2.25	2.5	2.75	V
Operation temperature	Topr	-20	25	60	℃
Storage temperature	Tstor	-40	25	80	℃

7.2 POWER CONSUMPTION

[Table 7-2] Power Consumption Table

Parameter	Symbol	Min	Typ.	Max	Units
Main Power	VCC_SYS				mA
BF30A Analog Power	VDD_3V3				mA
MS500 Flash Power	VDD_1V8			169	uA
eFuse power	MS_eFUSE_EN_2V5			2	mA

8 . MECHANICAL DATA

8.1 DIMENSION

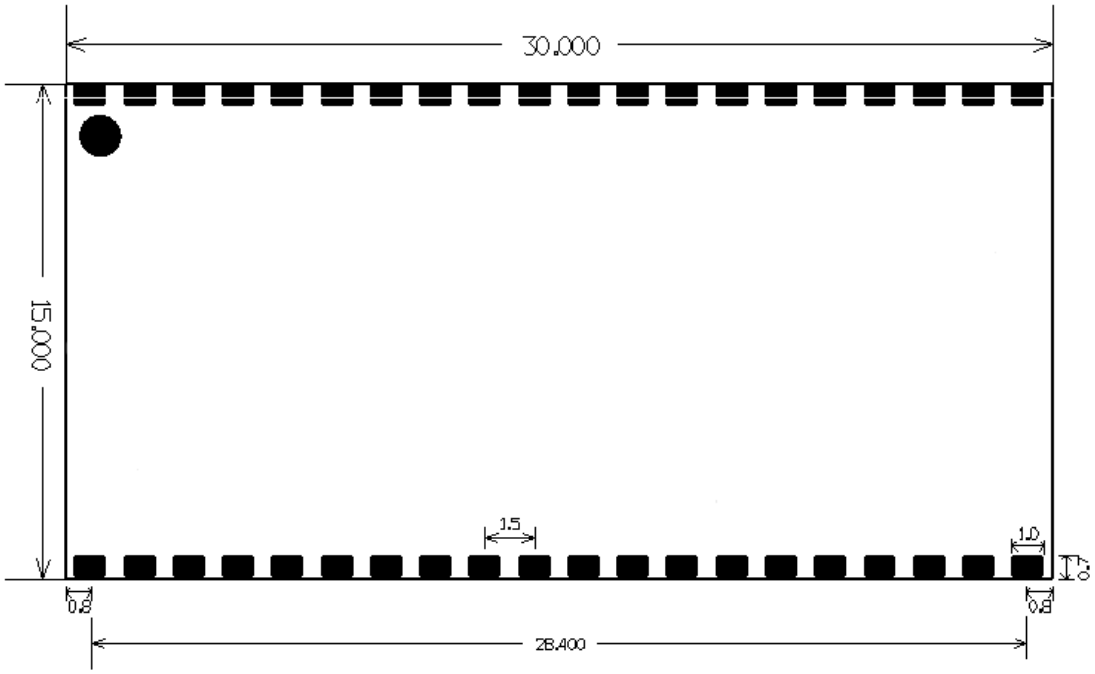


Figure 8-1. Top View

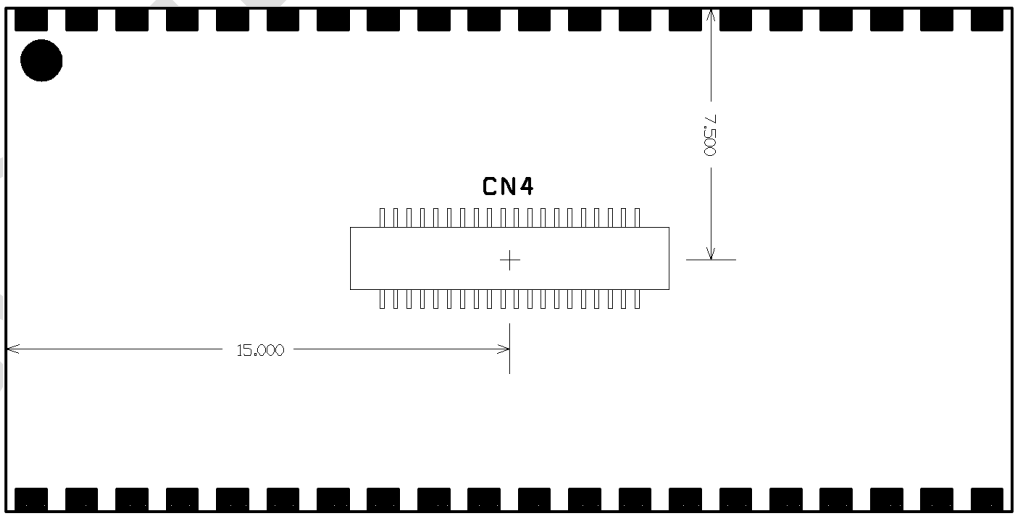


Figure 8-1. Bottom View

8.2 CONNETOR INFORMATION

Module Connector

- Connector Type: 0.4mm pitch Board to Board connector

  (Available Height: 1.5mm ~ 4.0mm Available)

- Manufacturer & Part Number: HIROSE DF40-Series (Refer to DF40_catalog.pdf of HIROSE)

●Receptacle

DF40 ❶ # ❷ - (**) ❸ - * ❹ DS ❺ - 0.4 ❻ V ❼ (**) ❽

❶ Series Name: DF40	❸ Stacking height	❹ No. of Contacts
❷ Style B : With reinforcing metal fitting HB : With reinforcing metal fitting (The H denotes a stacking height 2.5mm or above) C : Without reinforcing metal fitting HC : Without reinforcing metal fitting (The H denotes a stacking height 2.5mm or above)	Display / Stacking height None / 1.5mm 2.0 / 2.0mm 2.5 / 2.5mm 3.0 / 3.0mm 3.5 / 3.5mm 4.0 / 4.0mm	❺ Connector Type DS : Double row receptacle ❻ Contact Pitch : 0.4mm ❼ Mating direction Shape V : Vertical SMT ❽ Packaging Type (51) Embossed tape packaging

●Header

DF40 ❶ # ❷ * ❸ DP ❹ - 0.4 ❺ V ❻ (**) ❼

❶ Series Name : DF40	❸ No. of Contacts	❺ Contact Pitch : 0.4mm
❷ Style C : Without reinforcing metal fitting	❹ Connector Type DP : Double row pin header	❻ Mating direction V : Vertical SMT ❼ Packaging Type (51) Embossed tape packaging

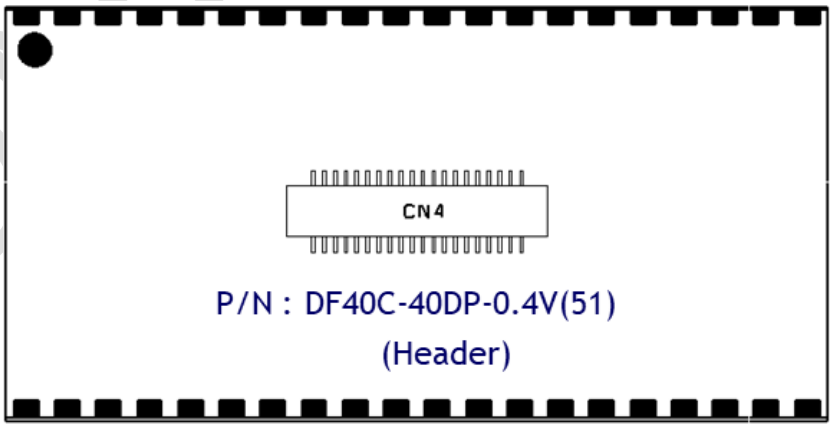


Figure 8-2. Connector Information

8.3 PRODUCT DESCRIPTION

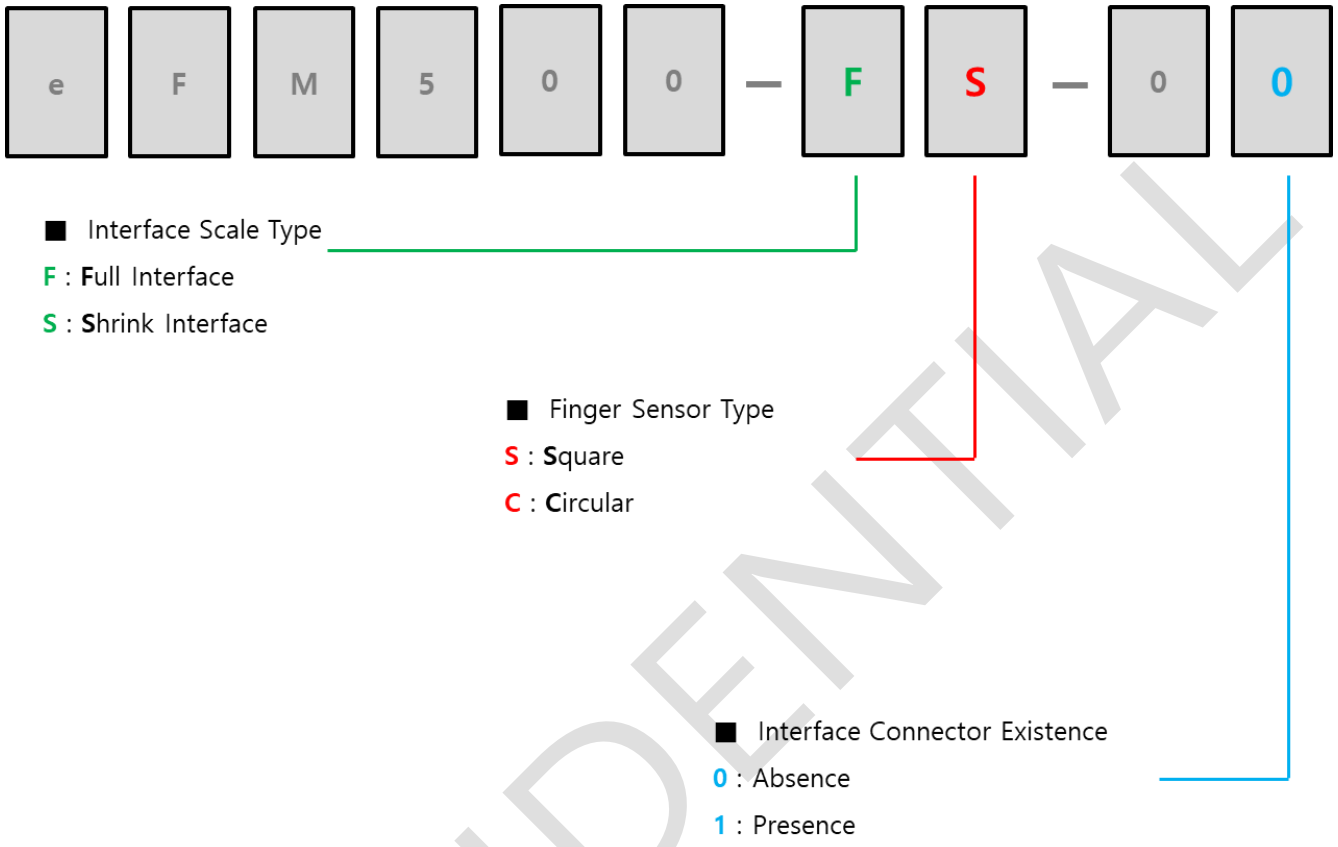


Figure 8-3. Product Description

COPYRIGHT NOTICE

NO WARRANTY NOTICE

eWBM Co., Ltd. makes no warranty of any kind in regard to this material which is delivered to you as is, including, but not limited to, the implied warranties as to its accuracy or fitness for a specific purpose. Any use of this technical documentation or the information contained therein is at the risk of the user. eWBM Co., Ltd. shall not be liable for errors contained therein or for incidental consequential damages in connection with the furnishing, performance or use of the material.

The information contained in this document is subject to change without notice.