Specification No. 3-1308-8746-1900

PDI
PCI HEAD
MMD-1900

Secure Magnetic

Assy Head for PCI Compliance
AES Encryption
DUKPT Key Management

Interface

SPI, UART

Reads and Encrypts up to Three Tracks, Ideal for PCI POI 3.0

For Product information, application engineering assistance or pricing, contact us at:

Peripheral Dynamics Inc.
5150 Campus Drive
Plymouth Meeting, PA 19462-1123

Specification No. 3-1308-8746-1900

Toll Free: 800-523-0253
Phone: 610-825-7090 Fax: 610-834-7708
Email: sales@pdiscan.com Internet: www.pdiscan.com

November 13, 2013

CONTENTS

1. Introduction

1.1. Overview

MMD1900 integrates the magnetic card reader function with data encryption. Upon reception of the magnetic head signals, the card data is recovered, encrypted, and transferred to the external device via universal asynchronous receiver and transmitter (UART) or serial peripheral interface (SPI).
It supports up to 3 track card reading at the same time. Signal processing techniques are employed to recover F2F encoded data reliably from head signals with severe fluctuation of signal amplitude, widely varying bit interval, and jittery bit position. The recovered data is encrypted with the 128 bit AES.

Fig. 1 shows the simplified block diagram of MMD-1900.

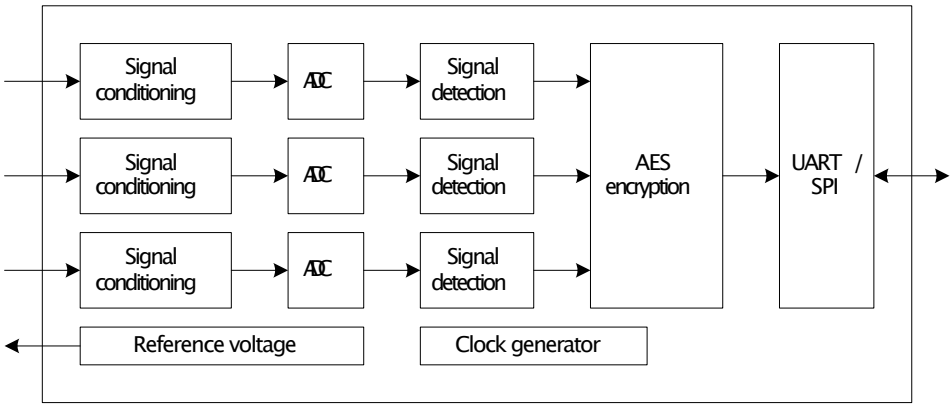


Figure 1: Block diagram

1.2. Features

- All electronics are potted inside the head to prevent tampering
- All card data from the head is encrypted
- Full three tracks Support
- Signal Conditioning Adapted to Head Signal
- Digital Signal Processing for Superior Data Recovery Performance
- Secure Data Transfer with **128 bit AES Encryption**: CBC Mode
- **DUKPT key management** (Derived Unique Key Per Transaction)
- ISO/IEC 7811 and Binary Data Format Support
- Flexible External Interface: UART or SPI
- Power Down Mode for Low Power Consumption
- Wide range of card swipe speed : from 5 to 150 cm/s

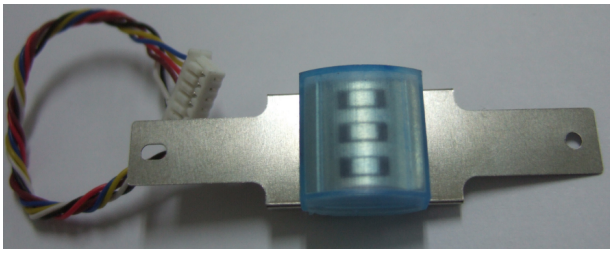
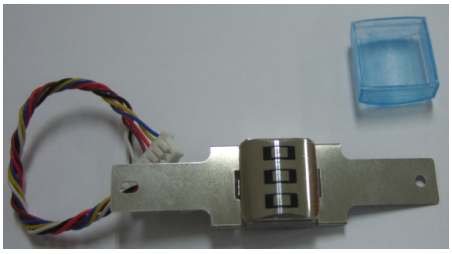
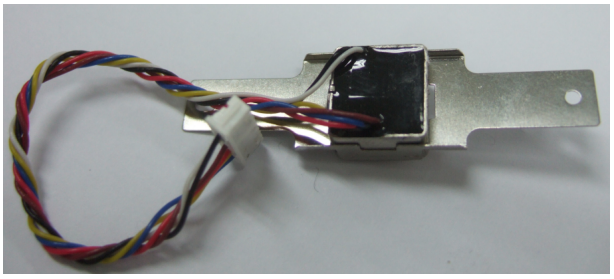
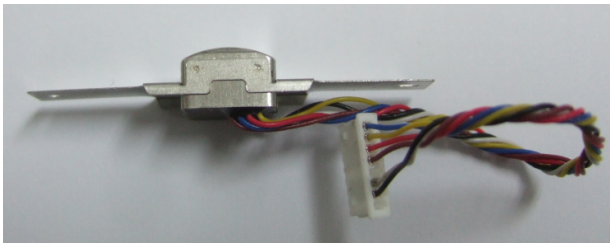
1.3. Applications

- POS (Point of Sales) Terminal
- ATM Machine
- Card Key Entry System
- Card reader for security system

2. External Interface & Picture

SPI : 6pin (recommended for future upgrade without HW change)
UART : 4pin

<Tip>
100% HW Compatible with Magtek's Intelli-head and need only small part of Software Program change, if the user is already using Magtek's.
For this job, SDK (Software Development Kit) and development source can be provided.

- SPI interface cable pin out
  Connector Housing : Molex (part#51021-0800)

Conn#	COLOR	SIGNAL
1 PIN	BLUE	SPI_CLOCK
2 PIN	YELLOW	SDO(TXD)
3 PIN	RED	SDI(RXD)
4 PIN	BROWN	DATA_RDY
5 PIN	N/A	N/A
6 PIN	WHITE	VDD(3.3V)
7 PIN	BLACK	GND
8 PIN	N/A	N/A

3. Functional Description

1. Signal Conditioning and Processing

The head signal input is amplified to fit the signal amplitude to the dynamic range of the circuit and filtered to remove the out of band noise before digital signal processing. The analog to digital converter (ADC) digitizes the incoming signal to generate a digital signal. The digital signal processing techniques adopted include acquisition and tracking of widely varying bit interval, signal amplitude tracking, minimizing jitter of bit position, removal of false peak and zero crossing, and sequential detection of F2F encoded data. The implemented analog signal conditioning and digital signal processing technology demonstrates a superior performance in the recovery of the magnetic card data.

2. Encryption

The recovered card data can be encrypted by the 128 bit AES before transferring to the external device. The implementation supports CBC mode. For the improved security, the derived unique key per transaction (DUKPT) key management scheme is supported. The initial key setting, encryption mode selection, data encryption, and transfer of the encrypted data are conducted via the commands through the external data interface, UART or SPI, as explained in the Command section.

3. SPI or UART Interface

The external data interface either UART or SPI is selected by the state of the SPI_CLK input pin. The UART interface is selected as long as the SPI_CLK stays at the logical high state (3.3v) after the external reset signal input (RESETB=0V) or the power down (VDD=0V or PD=3.3V). The SPI interface is selected if the SPI_CLK is at the logical low state (0V) at least 3usec period after the external reset signal or the power down. Once the SPI is chosen, the SPI is assumed until the next external reset signal input or the power down.
The UART interface supports the baud rate of 9.6, 19.2kbps. The frame structure is shown in Fig. 2. One start bit and at least one stop bit should be included in the frame. The data word consists of 8 bits. The LSB of the data is transmitted first. (1 start bit + 8 data bits, 1 stop bit, none parity).

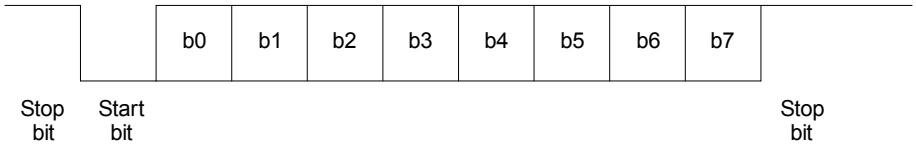


Figure 2: Frame Format of UART Interface.

The SPI interface uses SPI_CLK input as the timing reference to transmit or receive data through TXD and RXD, respectively. The supported data rate is from 10kbps to 100kbps. The data transmit and receive timing diagrams are shown in Fig. 3 and 4, respectively. The DATA_RDY output pin is asserted to notify the external device of the data availability. Once the DATA_RDY is asserted, the external device provides SPI_CLK to the chip and can latch the TXD signal at the falling edge of SPI_CLK. The chip receives bits through RXD and latches the signal at the falling edge of the SPI_CLK. Note that if there is no SPI_CLK input for 500msec after the DATA_RDY assertion, the DATA_RDY signal is de-asserted.

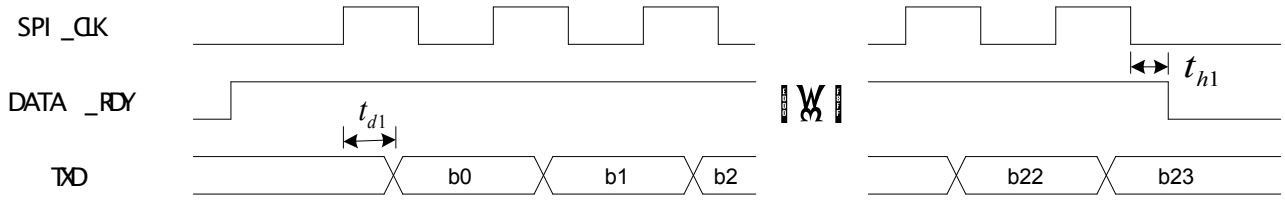


Figure 3: Timing diagram of SPI transmit data.

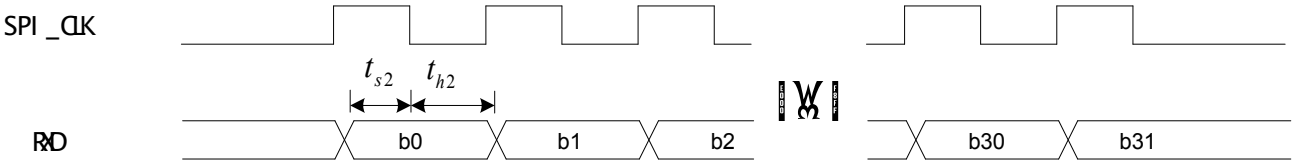


Figure 4: Timing diagram of SPI receive data.

4. Commands

Various commands are implemented to read data out of the chip, to set the initial encryption key and the operating mode of the chip, etc. These commands are provided to the chip via the UART or SPI. The response from the chip to each command can be used to check the effectiveness of the command.
The command from the external device to the chip consists of the various fields as shown below.

Command format

STX (1byte)	Class (1byte)	Function (1byte)	Length (1byte)	TX Data (n byte)	ETX (1byte)	BCC (1byte)

* STX : Command Start Character (0x02)
* Class : Class of command
* Function : Requested function for the chip to conduct
* Length : Number of bytes in Data field
* TX Data : Data
* ETX : End Character (0x03)
* BCC : Check Sum (Exclusive OR value from STX to ETX)

Response format

STX (1byte)	Class (1byte)	Function (1byte)	Length (1byte)	Status (1byte)	RX Data (n byte)	ETX (1byte)	BCC (1byte)

* STX : Start Character for Response (0x02)
* Class : Re-transmission of the Class sent in the command
* Function : Re-transmission of the Function sent in the command
* Length : Number of bytes in RX Data field
* Status : Status Check Byte
  ACK (0x06): Successful execution of the command
  NAK (0x15): Failed execution of the command
* RX Data : Response Value and error code as response
* ETX : End Character for response (0x03)
* BCC : Check sum (Exclusive OR value from STX to ETX)

The commands are listed in Table 1.

Table 1: List of Commands

Type	Class	Function	Length	Data	Remark

Get Version	0x10	0x31	0x00	-	Retrieve the version information of the chip
Load AES Parameters	0x11	0x31	0x1A	Key Serial Number (10 bytes), Initial Key (16 bytes)	Load AES key serial number and initial key to the chip
Load User Parameters	0x12	0x31	0x04	TX Mode (1byte), VGA Gain (1byte), All Track Error (1byte), KSN Response (1byte)	Set the operating mode of the chip
UART Calibration	0x13	0x31	0x05	0xAAAAAAAAAA (5byte)	UART calibration
Load Initialization Vector	0x14	0x31	0x10	Initial Vector (16 bytes)	Load AES initialization vector
OTP Write (AES Parameter)	0x15	0x31	0x00	-	OTP write of AES parameters **(OTP write maximum 2 times)**
OTP Write (User Parameter)		0x32	0x00	-	OTP write of user parameters **(OTP write maximum 2 times)**
OTP Write (UART calibration)		0x33	0x00	-	OTP write of UART calibration result **(OTP write maximum 4 times)**
Get Status	0x16	0x31	0x00	-	Get the current setting of the chip
Read Data Retry	0x17	0x31	0x00	-	Re-read the data frame retrieved the most recent
Software Reset	0x18	0x31	0x00	-	Initialize the chip

<Note> It takes 50ms to complete the command.

The responses to the commands are listed in Table 2.

Table 2: List of Responses

Type	Class	Function	Length	Status	Data	Remark
Get Version	0x10	0x31	0x10	0x06	MMD1000 VER:1.00	Current chip versions information return
			0x01	0x15	Error Code	Error code return

Load AES Parameter	0x11	0x31	0x0D	0x06	KSN (10 bytes) KCV (3 bytes)	AES key serial number and Key check value return
			0x01	0x15	Error Code	Error code return
Load User Parameter	0x12	0x31	0x04	0x06	TX Mode (1byte) VGA Gain (1byte) All Track Error (1byte) KSN Response (1byte)	Current operating mode return
			0x01	0x15	Error Code	Error code return
UART Calibration	0x13	0x31	0x01	0x06	Calibration Value (1byte)	UART calibration result return
			0x01	0x15	Error Code	Error code return
Load Initialization Vector	0x14	0x31	0x03	0x06	KCV (3bytes)	Key check value return
			0x01	0x15	Error Code	Error code return
OTP Write (AES Parameter)	0x15	0x31	0x0D	0x06	KSN (10bytes), KCV (3bytes)	Key serial number and Key check value OTP write
			0x01	0x15	Error Code	Error code return
OTP Write (User Parameter)		0x32	0x04	0x06	TX Mode (1byte) VGA Gain (1byte) All Track Error (1byte) KSN Response (1byte)	User parameters OTP write
			0x01	0x15	Error Code	Error code return
OTP Write (UART calibration)		0x33	0x01	0x06	Calibration Value (1byte)	UART calibration result OTP write
			0x01	0x15	Error Code	Error code return
Get Status	0x16	0x31	0x06	0x06	TX Mode (1byte) VGA Gain (1byte) All Track Error (1byte) KSN Response (1byte) Reserved (1byte) UART Calibration (1byte)	Current setting information return
			0x01	0x15	Error Code	Error code return
Read Data Retry	Un-encrypted Most Recent Data Frame					Re-read of the most recent un-encrypted data frame
	0x17	0x31	0x01	0x15	Error Code	Error code return
Software Reset						No response for successful initialization
	0x18	0x31	0x01	0x15	Error Code	Error code return

- The error codes carried in the response TX Data field are summarized in Table 3.

Table 3: List of Error Codes

Error Code	Description
0x31	CRC error in encryption related information stored in OTP
0x32	No information stored in OTP related to encryption
0x41	AES initial vector is not set yet
0x51	Preamble error in card read data
0x52	Postamble error in card read data
0x53	LRC error in card read data
0x54	Parity error in card read data
0x55	Blank track
0x61	STX/ETX error in command communication
0x62	Class/Function un-recognizable in command
0x63	BCC error in command communication
0x64	Length error in command communication
0x65	No data available to re-read
0x71	No more space available for OTP write
0x72	OTP write try without data
0x73	CRC error in read data from OTP
0x74	No data stored in OTP

- The chip supports the following 6 data transmit mode (TX Mode).
- TX Mode should be set as follows before use it because we do not set this from our factory.

Table 4: Data Transmit Mode

TX Mode	Transmit Mode
MODE2(0x02)	Binary data format (binary low data LSB first)
MODE4(0x04)	Binary data encrypted without initial vector use
MODE6(0x06)	Binary data encrypted by using initial vector

- The all track error field can have one of the 2 settings as follows

Table 5: all track error response setting

all track error	all track error response setting
0x00	all track error report : Enabled - **default setting**
0x01	no all track error report : Disabled

- The key serial number response field sets the length of the key serial number in the response format as follows.

Table 6: key serial number response setting

KSN	key serial number response setting
0x00	10 byte key serial number reporting, **default setting**
0x01	3 byte(21bit encryption count) of key serial number reporting

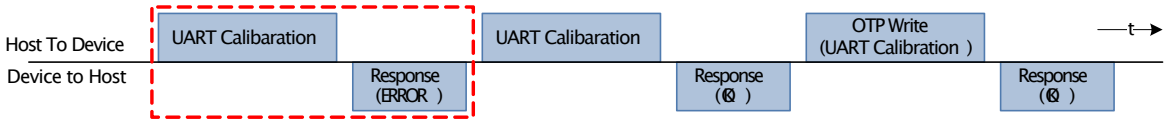
- To use the encryption, the initial key, key serial number, and data transmit mode should be set prior to the card swipe. Follow these steps to set the required information into the chip.

  Step 1: Command “load AES parameters” to the chip
  Step 2: Check the response from the chip
  Step 3: Command “OTP write (AES parameter)” to the chip
  Step 4: Check the response from the chip
  Step 5: Wait at least 500msec
  Step 6: Command “load user parameter” to set the data transmit mode to AES CBC
  Step 7: Check the response from the chip
  Step 8: Command “OTP write (User parameter)” to the chip
  Step 9: Check the response from the chip
  Step 10: Wait at least 500msec

- Note that after the command of “load AES parameter”, “load user parameter”, “UART calibration” the next command should be the corresponding “OTP Write” command followed. If the next command is not the “OTP Write”, then the response frame with an error code is generated in response to a command. The OTP write procedure should restart from the beginning with the command like “load AES parameter”, “load user parameter”, “UART calibration” The maximum number of OTP writes is 2 times for AES parameter and user parameter and 4 times for UART calibration

- If the “Software Rest” command is issued without any error, all the registers of the chip are set to their initial values and the initial key, key serial number, and user setting are retrieved from the OTP memory. The error type for the “Software Rest” command is limited to the communication error and unknown command error.

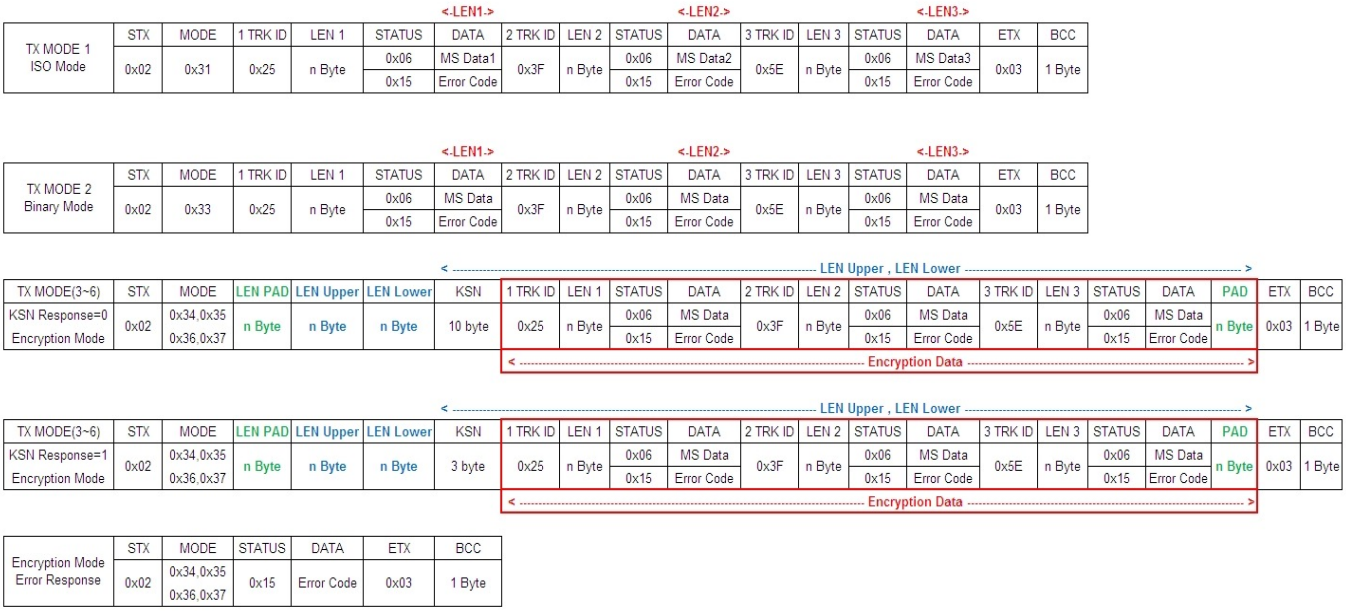
- To set the baud rate of the UART interface, use the “UART calibration” command as the first command after the power-up or reset. The chip will automatically tune the baud rate to the incoming bit period of the data field of the command (9.6kbps ~ 19.200kbps).



- In response to the “Read Data Retry” command, the chip transmits the most recent data read from the card. If the AES encryption mode is used, the chip does not retransmit the data even with the successful reception of the “Read Data Retry” command for the security reason.

- The lowest 21 bits of the key serial number in the “Load AES parameter” command are not used in the chip. However, the response to the “Load key serial number” command include the same 21 bits values as in the command. These 21 bits are reserved for the encryption counter (or transaction counter) value for the DUKPT. The lowest 21 bits of the key serial number field of the encrypted data frame contains this encryption counter value.

- The data frame formats are shown in Fig. 5.



						<-LEN1->				<-LEN2->				<-LEN3->			
TX MODE 1 ISO Mode	STX	MODE	1 TRK ID	LEN 1	STATUS	DATA	2 TRK ID	LEN 2	STATUS	DATA	3 TRK ID	LEN 3	STATUS	DATA	ETX	BCC
	0x02	0x31	0x25	n Byte	0x06	MS Data1	0x3F	n Byte	0x06	MS Data2	0x5E	n Byte	0x06	MS Data3	0x03	1 Byte
					0x15	Error Code			0x15	Error Code			0x15	Error Code		

						<-LEN1->				<-LEN2->				<-LEN3->			
TX MODE 2 Binary Mode	STX	MODE	1 TRK ID	LEN 1	STATUS	DATA	2 TRK ID	LEN 2	STATUS	DATA	3 TRK ID	LEN 3	STATUS	DATA	ETX	BCC
	0x02	0x33	0x25	n Byte	0x06	MS Data	0x3F	n Byte	0x06	MS Data	0x5E	n Byte	0x06	MS Data	0x03	1 Byte
					0x15	Error Code			0x15	Error Code			0x15	Error Code		

							<- LEN Upper , LEN Lower ->												
TX MODE(3~6)	STX	MODE	LEN PAD	LEN Upper	LEN Lower	KSN	1 TRK ID	LEN 1	STATUS	DATA	2 TRK ID	LEN 2	STATUS	DATA	3 TRK ID	LEN 3	STATUS	DATA	PAD	ETX	BCC
KSN Response=0 Encryption Mode	0x02	0x34,0x35 0x36,0x37	n Byte	n Byte	n Byte	10 byte	0x25	n Byte	0x06	MS Data	0x3F	n Byte	0x06	MS Data	0x5E	n Byte	0x06	MS Data	n Byte	0x03	1 Byte
									0x15	Error Code			0x15	Error Code			0x15	Error Code			
							<- Encryption Data ->												

							<- LEN Upper , LEN Lower ->												
TX MODE(3~6)	STX	MODE	LEN PAD	LEN Upper	LEN Lower	KSN	1 TRK ID	LEN 1	STATUS	DATA	2 TRK ID	LEN 2	STATUS	DATA	3 TRK ID	LEN 3	STATUS	DATA	PAD	ETX	BCC
KSN Response=1 Encryption Mode	0x02	0x34,0x35 0x36,0x37	n Byte	n Byte	n Byte	3 byte	0x25	n Byte	0x06	MS Data	0x3F	n Byte	0x06	MS Data	0x5E	n Byte	0x06	MS Data	n Byte	0x03	1 Byte
									0x15	Error Code			0x15	Error Code			0x15	Error Code			
							<- Encryption Data ->												

	STX	MODE	STATUS	DATA	ETX	BCC
Encryption Mode Error Response	0x02	0x34,0x35 0x36,0x37	0x15	Error Code	0x03	1 Byte

Figure 5: TX Data frame format

- The data format is determined by the TX Mode setting. The mode field of the data frame is generated by 0x31 + TX Mode. The “LEN PAD” is the length of the padded data (“PAD” field) at the end of the data to make the encrypted block the multiple of 128 bits.

4. Electrical Characteristics

4.1. Absolute Maximum Ratings

Parameter	Symbol	Limits	Units
Supply Voltage	VDD	-0.3 to +3.6	V
Input Voltage	VIN	-0.3 to VDD+0.3	V
Storage Temperature	ST	-65 to +150	℃
Maximum Junction Temperature	MJT	-20 to 125	℃

4.2. Operating Conditions

Parameter	Symbol	Minimum	Typical	Maximum	Units
Supply voltage	VDD	3.0	3.3	3.6	V
Operating Temperature	OT	-20		+70	℃

4.3. DC Electrical Characteristics

Parameter	Symbol	Minimum	Typical	Maximum	Units	Test Conditions
Input Voltage High	V	2.0	-	3.6	V	

Input Voltage Low	V	-0.3	-	0.8	V	
Output Voltage High	V	2.4	-	3.6	V	I_{OH}
Output Voltage Low	V	0.0	-	0.4	V	I_{OL}
Input Current	I_I	-1	-	1	uA	
VDD Supply Current (normal mode)	I_{DD}	-	1.7	2	mA	PD=0V
LDO Output Voltage	V_{LDO}	1.6	1.8	2.0	V	VDD=3.3V
VREF Voltage	V_{vref}	1.0	0.9	0.8	V	VDD=3.3V

4.4 AC Electrical Characteristics

Parameter	Symbol	Minimum	Typical	Maximum	Units	Test Conditions
TXD signal delay	t_{d1}	-	-	3	usec	SPI interface mode
DATA_RDY hold time	t_{h1}	2	-	-	usec	SPI interface mode
RXD setup time	t_{s2}	1	-	-	usec	SPI interface mode
RXD hold time	t_{h2}	3	-	-	usec	SPI interface mode

<NOTE>

**** 90mm rail (frame) version is also available (Model name: MMD-1901) please refer to the dimensions on next page.*

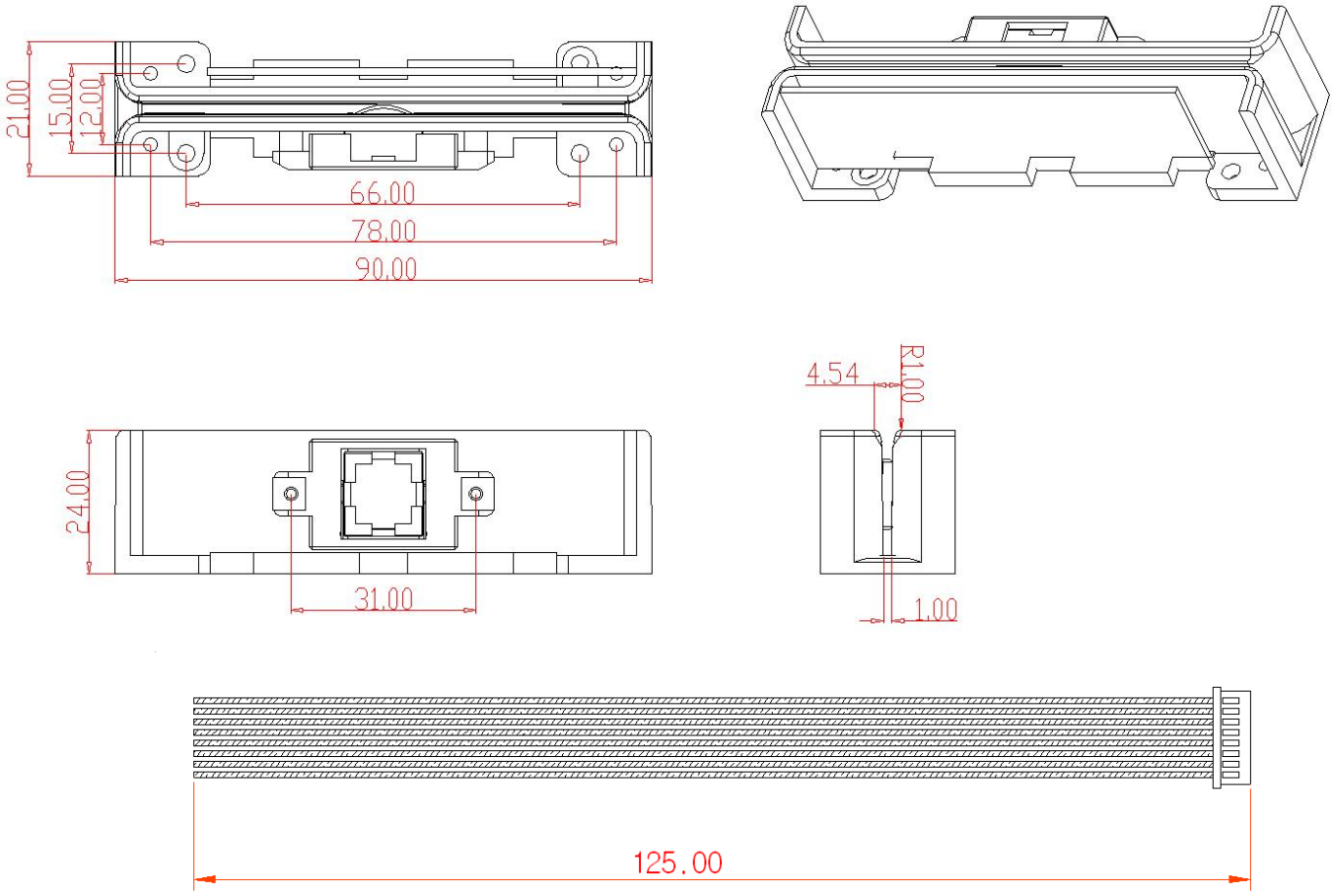
**** 43mm rail (frame) version is also available (Model name: MMD-1902) please refer to the dimensions on next page.*

**** Customized "Cushion spring (head bracket)" for "Rail (frame)" is also possible butt please send us the drawing.*

**** The information contained in this document can be changed without notice.*

5 < Model name "MMD-1901": 90mm rail (frame) version dimensions >

Specification No. 3-1308-8746-1900



< Model name "MMD-1902" : 43mm slim rail (frame) version dimensions >

Will be updated.