W74M01GV

3V 1G-BIT
SERIAL FLASH MEMORY WITH
DUAL/QUAD SPI & SECURE AUTHENTICATION

Publication Release Date: February 17, 2017

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com
微信扫码咨询客服

winbond

Table of Contents

1. GENERAL DESCRIPTIONS 3
2. FEATURES 3
3. PACKAGE TYPES AND PIN CONFIGURATIONS 4
   - 3.1 Pad Configuration WSON 8x6-mm 4
   - 3.2 Pad Description WSON 8x6-mm 4
4. PIN DESCRIPTIONS 5
   - 4.1 Chip Select (/CS) 5
   - 4.2 Serial Data Input, Output and IOs (DI, DO and IO0, IO1, IO2, IO3) 5
   - 4.3 Write Protect (/WP) 5
   - 4.4 HOLD (/HOLD) 5
   - 4.5 Serial Clock (CLK) 5
5. BLOCK DIAGRAMS 6
   - 5.1 Operation Diagram 6
   - 5.2 Functional Block Diagram 6
6. FUNCTIONAL DESCRIPTIONS 7
   - 6.1 Authentication Flash Operations 7
     - 6.1.1 Authentication Flash Initialization 7
     - 6.1.2 Authentication Flash Operation Flow 8
     - 6.1.3 Operations Allowed / Disallowed to Authentication Flash 9
     - 6.1.4 Authentication Flash Status Register Definition 10
   - 6.2 Instruction Set Tables 11
     - 6.2.1 Instruction Set Table 2-1 (Authentication Flash Input Instruction, OP1)(1) 11
     - 6.2.2 Instruction Set Table 2-2 (Authentication Flash Output Instruction, OP2)(1) 11
     - 6.2.3 Instruction Set Table 2-3 (Authentication Flash Reset Instruction)(1) 11
   - 6.3 Instruction Descriptions 12
     - 6.3.1 Write Root Key Register (9Bh + 00h) 12
     - 6.3.2 Update HMAC Key (9Bh + 01h) 13
     - 6.3.3 Increment Monotonic Counter (9Bh + 02h) 14
     - 6.3.4 Request Monotonic Counter (9Bh + 03h) 15
     - 6.3.5 Reserved Authentication Flash Device Commands (9Bh + 04h~FFh) 15
     - 6.3.6 Read Authentication Flash Device Status / Data (96h) 16
     - 6.3.7 Enable Reset (66h) and Reset Device (99h) 17
7. ELECTRICAL CHARACTERISTICS(1) 18
   - 7.1 Absolute Maximum Ratings (2) 18
   - 7.2 Operating Ranges 18
   - 7.3 Power-Up Power-Down Timing and Requirements 19
   - 7.4 DC Electrical Characteristics(1) 20
   - 7.5 AC Measurement Conditions 21
   - 7.6 AC Electrical Characteristics(3,4) 22
   - 7.7 Serial Output Timing Diagram 24
   - 7.8 Serial Input Timing Diagram 24

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

8. PACKAGE SPECIFICATIONS 25
8.1 8-Pad WSON 8x6-mm (Package Code ZE) 25
8.2 Ordering Information 26
8.3 Valid Part Numbers and Top Side Marking 27
9. GENERAL INSTRUCTIONS 27
10. REVISION HISTORY 28

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

1. GENERAL DESCRIPTIONS

The W74M01GV (1G-bit) Serial Flash memory provides a storage solution for systems with limited space, pins and power. The W74 series offers flexibility and performance well beyond ordinary Serial Flash devices. They are ideal for code shadowing to RAM, executing code directly from Dual/Quad SPI (XIP) and storing voice, text and data. The device operates on a single 2.7V to 3.6V power supply with current consumption as low as 1µA for power-down. All devices are offered in space-saving packages.

The W74M01GV supports the standard Serial Peripheral Interface (SPI), Dual/Quad I/O SPI: Serial Clock, Chip Select, Serial Data I/O0 (DI), I/O1 (DO), I/O2 (/WP), and I/O3 (/HOLD). The device also provides a new Continuous Read Mode that allows for efficient access to the entire memory array with a single Read command. This feature is ideal for code shadowing applications.

The device supports JEDEC standard manufacturer and device ID, one 2,048-Byte Unique ID page, one 2,048-Byte parameter page and ten 2,048-Byte OTP pages. To provide better NAND flash memory manageability, user configurable internal ECC, bad block management are also available in W74M01GV.

The W74M product line includes a standard Hash-based Message Authentication Code (HMAC) SHA-256 crypto accelerator that is used for key establishment between devices or systems for secure authentication. Secure authentication is accomplished by using Root Keys and session based, HMAC Keys secretly shared between the host and the flash memory.

Each W74M device is equipped with four sets of non-volatile 256-bit for storing Root Keys; four sets of volatile 256-bit for storing HMAC Keys and four sets of non-volatile 32-bit for storing Monotonic Counter values. The four sets allows one device pairing up to four different Hosts. A Host can be another device, like a microprocessor, or a system.

Each Monotonic Counter, paired with a host, share a unique counter value (N) that can increment, N+1. The Host dictates the random number and incremental rate at the start of its first pairing. The constant changing counter value is a method to combat device counterfeiting and Replay attacks.

2. FEATURES

- **New Family of SpiFlash Memories**
  - W74M01GV: 1G-bit / 128M-byte
  - Page size 2,112 bytes (2048 + 64 bytes)
  - Block size 64 pages (128K + 4K bytes)
  - Standard SPI: CLK, /CS, DI, DO, /WP, /Hold
  - Dual SPI: CLK, /CS, IO_0, IO_1, /WP, /Hold
  - Quad SPI: CLK, /CS, IO_0, IO_1, IO_2, IO_3
  - Compatible SPI serial flash commands
- **Organization**
  - Density: 1G-bit/128M-byteHighest Performance of Serial NAND Flash
  - 104MHz Standard/Dual/Quad SPI clocks
  - 208/416MHz equivalent Dual/Quad SPI
  - 50MB/S continuous data transfer rate
  - Fast Program/Erase performance
  - More than 100,000 erase/program cycles
  - More than 10-year data retention
- **Low Power Serial Flash**
  - Single 2.7 to 3.6V supply
  - 25mA active, 10µA standby current
  - -40°C to +85°C operating range
- **Flexible Architecture with 128KB blocks**
  - Uniform 128K-Byte Block Erase
  - Flexible page data load methods
- **Advanced Security Features**
  - Integrated HMAC-SHA-256 Engine
  - 4 sets of 256-bit OTP Root Key
  - 4 sets of 256-bit volatile HMAC Key
  - 4 sets of 32-bit Monotonic Flash Counter
  - On chip 1-Bit ECC for memory array
  - ECC status bits indicate ECC results
  - bad block management and LUT(2) access
  - 2KB Unique ID and 2KB parameter pages
  - Ten 2KB OTP pages
  - Software and Hardware Write-Protect
  - Power Supply Lock-Down and OTP protection
- **Space Efficient Packaging**
  - 8-pad WSON 8x6 mm
  - Contact Winbond for other options

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

3. PACKAGE TYPES AND PIN CONFIGURATIONS

3.1 Pad Configuration WSON 8x6-mm

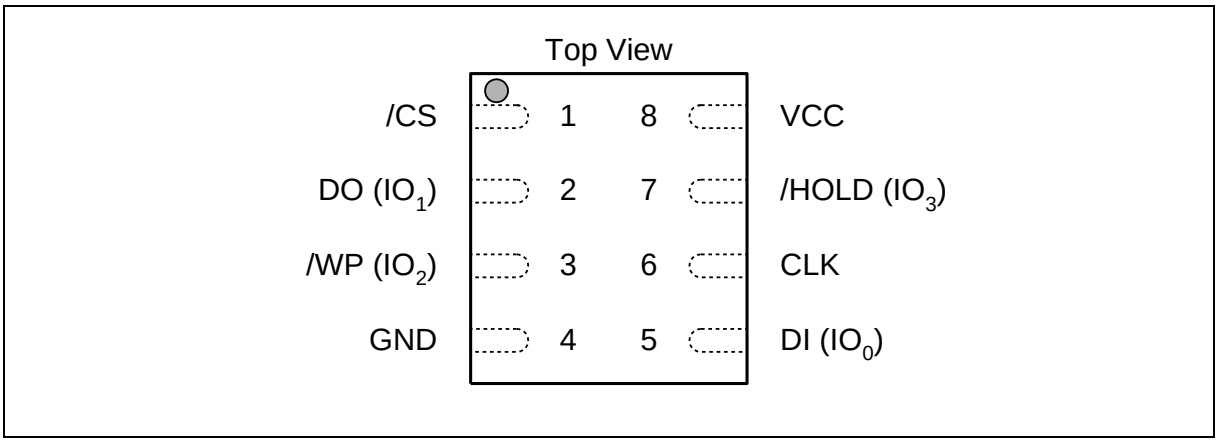


Figure 1a. W74M01GV Pad Assignments, 8-pad WSON 8x6-mm (Package Code E)

3.2 Pad Description WSON 8x6-mm

PAD NO.	PAD NAME	I/O	FUNCTION
1	/CS	I	Chip Select Input
2	DO (IO1)	I/O	Data Output (Data Input Output 1)(1)
3	/WP (IO2)	I/O	Write Protect Input (Data Input Output 2)(2)
4	GND		Ground
5	DI (IO0)	I/O	Data Input (Data Input Output 0)(1)
6	CLK	I	Serial Clock Input
7	/HOLD (IO3)	I/O	Hold Input (Data Input Output 3)(2)
8	VCC		Power Supply

Notes:

1. IO0 and IO1 are used for Standard and Dual SPI instructions
2. IO0 – IO3 are used for Quad SPI instructions, /WP & /HOLD functions are only available for Standard/Dual SPI.

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

4. PIN DESCRIPTIONS

4.1 Chip Select (/CS)

The SPI Chip Select (/CS) pin enables and disables device operation. When /CS is high the device is deselected and the Serial Data Output (DO, or IO0, IO1, IO2, IO3) pins are at high impedance. When deselected, the devices power consumption will be at standby levels unless an internal erase, program or write status register cycle is in progress. When /CS is brought low the device will be selected, power consumption will increase to active levels and instructions can be written to and data read from the device. After power-up, /CS must transition from high to low before a new instruction will be accepted. The /CS input must track the VCC supply level at power-up and power-down (see "Write Protection" and Figure 10a & 10b). If needed a pull-up resister on the /CS pin can be used to accomplish this.

4.2 Serial Data Input, Output and IOs (DI, DO and IO0, IO1, IO2, IO3)

The W74M01GV supports standard SPI, Dual SPI, Quad SPI operation. Standard SPI instructions use the unidirectional DI (input) pin to serially write instructions, addresses or data to the device on the rising edge of the Serial Clock (CLK) input pin. Standard SPI also uses the unidirectional DO (output) to read data or status from the device on the falling edge of CLK.

Dual/Quad SPI instructions use the bidirectional IO pins to serially write instructions, addresses or data to the device on the rising edge of CLK and read data or status from the device on the falling edge of CLK.

4.3 Write Protect (/WP)

The Write Protect (/WP) pin can be used to prevent the Status Register from being written. Used in conjunction with the Status Register's Block Protect bits BP[3:0] and Status Register Protect SRP bits SRP[1:0], a portion as small as 256K-Byte (2x128KB blocks) or up to the entire memory array can be hardware protected. The WP-E bit in the Protection Register (SR-1) controls the functions of the /WP pin.

When WP-E=0, the device is in the Software Protection mode that only SR-1 can be protected. The /WP pin functions as a data I/O pin for the Quad SPI operations, as well as an active low input pin for the Write Protection function for SR-1. Refer to section 7.1.3 for detail information.

When WP-E=1, the device is in the Hardware Protection mode that /WP becomes a dedicated active low input pin for the Write Protection of the entire device. If /WP is tied to GND, all "Write/Program/Erase" functions are disabled. The entire device (including all registers, memory array, OTP pages) will become read-only. Quad SPI read operations are also disabled when WP-E is set to 1.

4.4 HOLD (/HOLD)

During Standard and Dual SPI operations, the /HOLD pin allows the device to be paused while it is actively selected. When /HOLD is brought low, while /CS is low, the DO pin will be at high impedance and signals on the DI and CLK pins will be ignored (don't care). When /HOLD is brought high, device operation can resume. The /HOLD function can be useful when multiple devices are sharing the same SPI signals. The /HOLD pin is active low.

When a Quad SPI Read/Buffer Load command is issued, /HOLD pin will become a data I/O pin for the Quad operations and no HOLD function is available until the current Quad operation finishes.

4.5 Serial Clock (CLK)

The SPI Serial Clock Input (CLK) pin provides the timing for serial input and output operations.

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

5. BLOCK DIAGRAMS

5.1 Operation Diagram

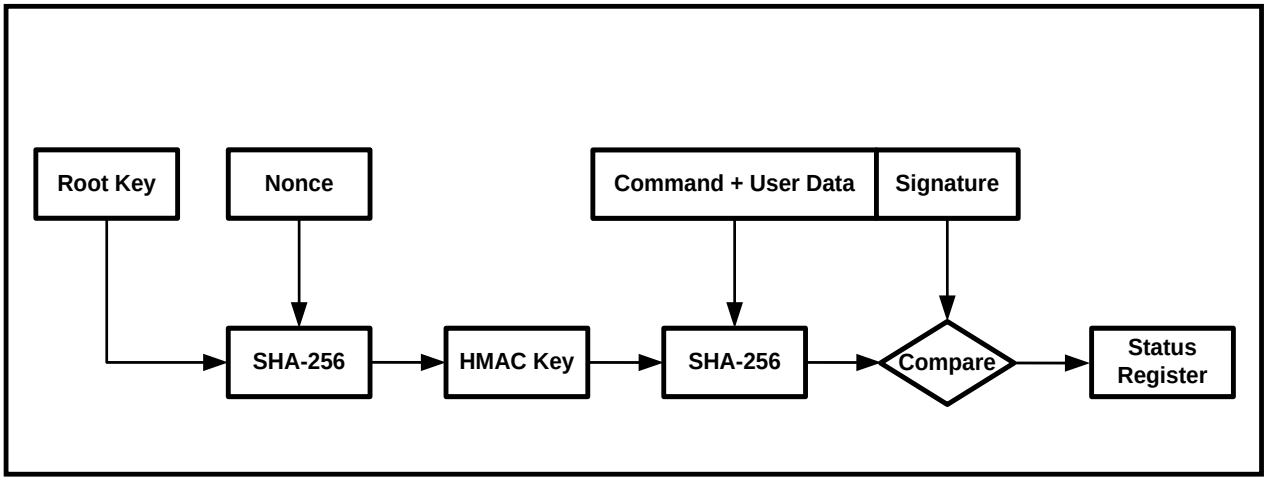


Figure 2. W74M01GV Operation Diagram

5.2 Functional Block Diagram

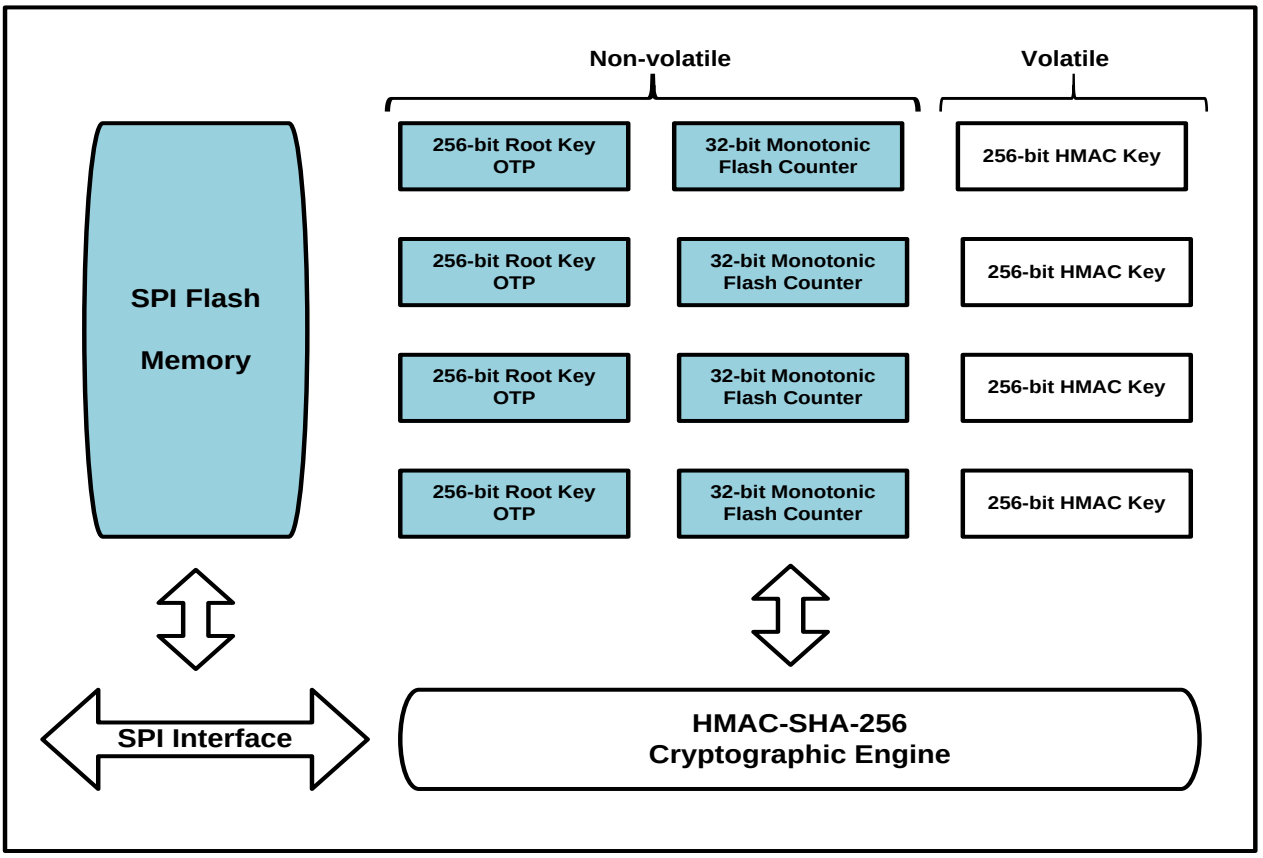


Figure 3. W74M01GV Functional Block Diagram

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

6. FUNCTIONAL DESCRIPTIONS

6.1 Authentication Flash Operations

The W74M01GV is equipped with four 32-bit Monotonic Counters. Each set is accessible by the 8-bit Counter_Address that is HMAC-signed by the appropriate secret key. The SPI Flash Host controller uses the Monotonic Counter value to validate authenticity of the attached W74M device or modules which the W74M device resides.

The Authentication operation is based on the HMAC-SHA-256 cryptographic algorithm. HMAC-SHA-256 is a type of keyed hash algorithm that is constructed from the SHA-256 hash function and used as a Hash-based Message Authentication Code (HMAC). The HMAC process mixes a secret key with the message data, hashes the result with the hash function, mixes that hash value with the secret key again, and then applies the hash function a second time. The output hash is 256 bits in length.

The HMAC can be used by two parties that share a secret key to ensure the transmitted message remains secure. The sender computes the hash value for the original data and then sends the hash value plus original data, as a single message, to the receiver. The receiver recalculates the hash value on the received message and compares the hash value with the one sent by the sender. The receiver then reports the result to the status register. Figure 2 in Section 5, demonstrates this process.

6.1.1 Authentication Flash Initialization

The Authentication Flash operation is initialized by issuing the “Write Root Key Register” command. When this command is successfully received and executed, a 256-bit Root Key will be written into the Authentication Flash permanently, and the corresponding Monotonic Counter will also be initialized to 0. After the initialization procedure, the Root Key value can no longer be altered or accessed externally through the SPI interface. The initialized Monotonic Counter is ready to accept the commands from the authentication SPI Flash HOST controller.

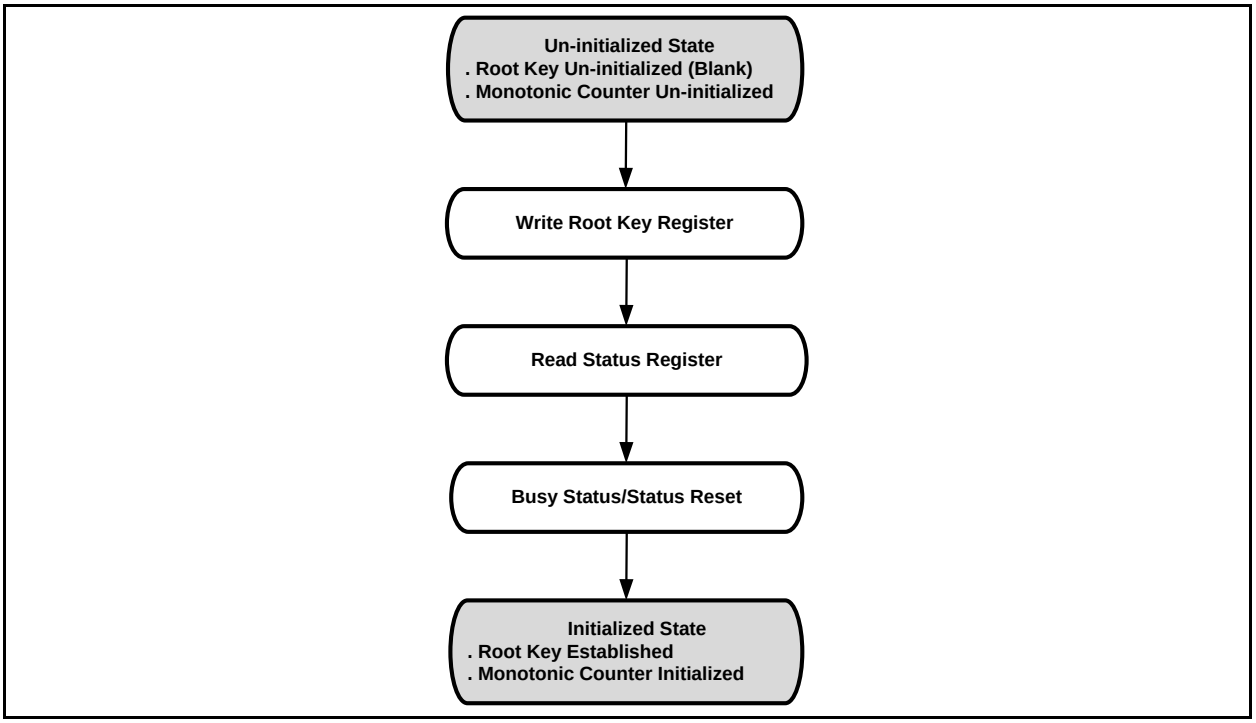


Figure 3a. W74M01GV Initialization Flow Diagram

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

6.1.2 Authentication Flash Operation Flow

Once the root key and the Monotonic Counter have been initialized, upon every power-up prior to any operations to Authentication Flash, the external SPI Flash HOST controller must update the HMAC Key register by issuing the “Update HMAC Key” command to W74M01GV Authentication Flash.

After initializing the HMAC key register, there are two different operations to perform: “Increment Monotonic Counter” command to increase the Monotonic Counter value by 1 and “Request Monotonic Counters” command to read out the value of the Monotonic Flash Counter.

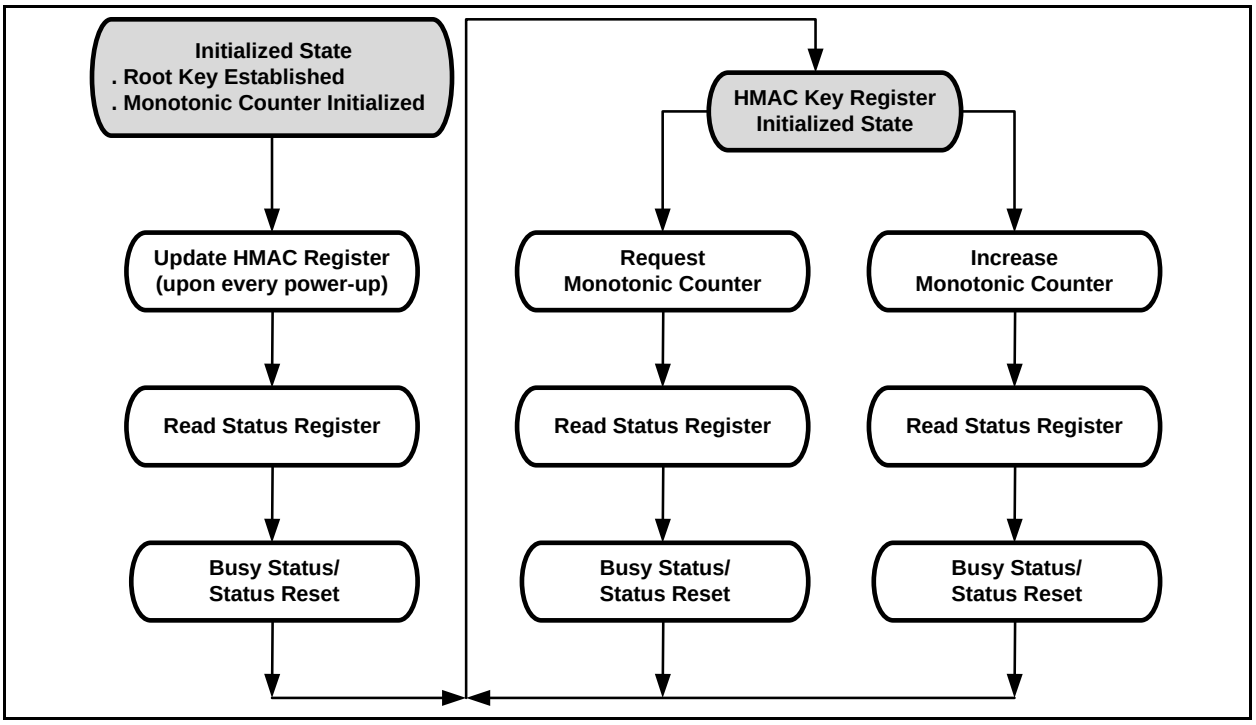


Figure 3b. W74M01GV Authentication Flash Operation Flow Diagram

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

6.1.3 Operations Allowed / Disallowed to Authentication Flash

The operation to Authentication Flash is independent to the standard SPI Flash operations. The input command OP1 (9Bh) dedicated to Authentication Flash will initial internal operations after the authenticated command is accepted by the device. During the internal operation period, the BUSY bit in the Authentication Flash Status Register (bit 0) will be set to 1. The Authentication Flash internal operation cannot be suspended and can only be interrupted by the Device Reset command (66h+99h). While the operations dedicated to Authentication Flash is going on, other standard SPI Flash commands can be issued and executed. Please refer to the table below for details.

Operations	Device Behavior
Authentication Flash OP1 command	The input command OP1 will be ignored while an operation to Authentication Flash is on-going.
Read Authentication Flash Status/Data OP2 command	The Status Register can be read out while an operation to Authentication Flash is on-going and this is the way to check if the operation has finished or not. If the BUSY bit of Status Register is set as 1, the data output following the Status Register is not valid.
Authentication Flash Device Reset	The software reset sequence can be issued any time during the internal operations of the Authentication Flash. All volatile settings will be reset.

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

6.1.4 Authentication Flash Status Register Definition

During the Authentication Flash operations, an 8-bit Status Register is used to indicate various states of the command execution and device status. A “Read Authentication Flash Status” command can be issued during any operation to check the Status Register.

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Successful Completion	Not Defined	Fatal Error (Pgm/Erase Fail or no valid counter found)	Monotonic_Counter_Data Mismatch	HMAC Key Reg Uninitialized	Signature Mismatch or Counter Address out of range or Write_Mode out of range	Root Keys Overwrite or Root Keys length mismatch or TruncatedSig Mismatch	BUSY

Authentication Flash Status Register[7:0]	Applicable CmdType(s)	Description
00000000	--	Power On State (Read Authentication Flash Status is issued directly after power-up).
10000000	00, 01, 02, 03	This status must be set on successful completion (no errors) of OP1 command (9Bh).
0xxxxxx1	00, 01, 02, 03, 04-FF	This bit must be set to 1, when device is busy executing OP1 command (9Bh). It is reset to 0 when the command execution is done.
0xxxxx1x	00, 01	This bit is set only when the correct payload size is received. For CmdType = 00, this bit must be set on Root Key Register Overwrite or Counter Address out of range or Truncated Signature mis-match error. For CmdType = 01, this bit is set when the corresponding Monotonic Counter is uninitialized.
0xxxx1xx	00, 01, 02, 03	This bit must be set on Signature Mismatch, Counter Address out of range when correct payload size is received; or CmdType is out of range; or incorrect payload size is received.
0xxx1xxx	02, 03	This bit must be set on HMAC Key Register (or Monotonic Counter) uninitialized on previous OP1 command when correct payload size is received.
0xx1xxxx	02	This bit must be set on Monotonic_Counter_Data Mismatch on previous increment when correct payload size is received.
0x1xxxxx	--	Fatal Error, e.g. program fail, no valid counter found after initialization.
Current value	--	Status register will naturally not be updated until first 8 bits of OP1 (9Bh) is received. However it is expected that the correct error type is reflected for any OP1 operation that exceeds a minimum of 16 clocks with active chip-select.

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

6.2 Instruction Set Tables

6.2.1 Instruction Set Table 2-1 (Authentication Flash Input Instruction, OP1)(1)

INSTRUCTION NAME	BYTE 0	BYTE 1 (CmdType)	BYTE 2	BYTE 3(2)		
Write Root Key Register	**9Bh**	**00h**	CounterAddr[7:0]	Reserved[7:0]	Byte 4 - 35 RootKey[255:0]	Byte 36 - 63 TruncatedSign[223:0]
Update HMAC Key Register	**9Bh**	**01h**	CounterAddr[7:0]	Reserved[7:0]	Byte 4 - 7 KeyData[31:0]	Byte 8 - 39 Signature[255:0]
Increment Monotonic Counter	**9Bh**	**02h**	CounterAddr[7:0]	Reserved[7:0]	Byte 4 - 7 CounterData[31:0]	Byte 8 - 39 Signature[255:0]
Request Monotonic Counter	**9Bh**	**03h**	CounterAddr[7:0]	Reserved[7:0]	Byte 4 - 15 Tag[95:0]	Byte 16 - 47 Signature[255:0]
Reserved Commands	**9Bh**	04h ~ FFh	Reserved			

6.2.2 Instruction Set Table 2-2 (Authentication Flash Output Instruction, OP2)(1)

INSTRUCTION NAME	BYTE 0	BYTE 1	BYTE 2	BYTE 3 - 14	BYTE 15 - 18	BYTE 19 - 50
Read Authentication Flash Status / Data(3)(4)	**96h**	Dummy	(Status[7:0])	(Tag[95:0])	(CounterData[31:0])	(Signature[255:0])

6.2.3 Instruction Set Table 2-3 (Authentication Flash Reset Instruction)(1)

INSTRUCTION NAME	BYTE 0	
Enable Reset	**66h**	
Reset	**99h**	

Notes:

1. All Authentication Flash instructions are in Standard SPI format. Each Input/Output Byte requires 8 clocks.
2. The Reserved[7:0] field for Authentication Flash OP1 must be all 0s (00000000'b).
3. The controller may terminate the Read Authentication Flash Status/Data instruction at any time without going through the entire data output sequence.
4. When BUSY=1, from Byte-3 and beyond, the device will output the Authentication Flash Status[7:0] value continuously until /CS terminates the instruction. The device will not output Tag, CounterData & Signature fields when BUSY=1. Once BUSY becomes 0, another OP2 command must be issued to read out the correct Tag, CounterData & Signature fields.

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

6.3 Instruction Descriptions

6.3.1 Write Root Key Register (9Bh + 00h)

This command is used by the SPI Flash HOST Controller to initialize the Root Key Register corresponding to the received Counter Address with the received Root Key. It is expected to be used in an OEM manufacturing environment when the SPI Flash HOST Controller and SPI Flash are powered together for the first time.

After the command is issued on the interface the Authentication Flash must ensure that the received transaction is error free. This includes checking following conditions:

- Payload size is correct. (including OP1 is 64 bytes)
- Counter Address falls within the range of supported counters.
- The Root Key Register corresponding to the requested Counter Address was previously uninitialized. [Root_Key_Reg_Init_State[Monotonic_Counter_Address] = 0xFFh]
- Truncated signature field is the same as least significant 224 bits of HMAC-SHA-256 based signature computed based on received input parameters.

If the received transaction is error free, the Authentication Flash successfully executes the command and posts “successful completion” in the Authentication Flash Status Register. This command must be executed to ensure that power cycling in the middle of command execution is properly handled. This requires that the internal state tracking the root key register initialization is written as the last operation of the command execution. (Root_Key_Reg_Init_State[Monotonic_Counter_Address] = 0]

Root Key Register Write with root key is = 256’hFF…FF is used as a temporary key. When this request is received error-free Root_Key_Reg_Init_State[Monotonic_Counter_Address] is not affected. Instead only the corresponding Monotonic Counter is initialized to 0 if previously uninitialized. This state is tracked as separate state using MC_Init_State[Monotonic_Counter_Address]. This state is used to leave the Monotonic Counter at the current value when an error free Root Key Register Write operation is received. (Both 256’hFF..FF and non 256’hFF..FF)

Once this command is successfully executed with a non 256’hFF..FF Root Key, the device will not accept the “Write Root Key Register” command any more, and the Root Key value cannot be read out by any instructions.

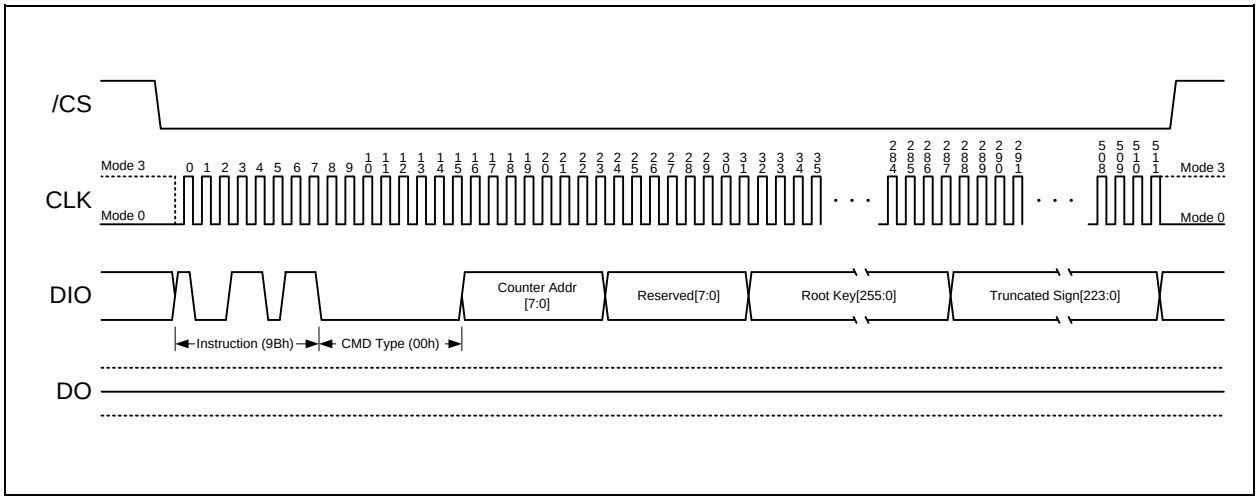


Figure 4. Write Root Key Register Instruction

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

6.3.2 Update HMAC Key (9Bh + 01h)

This command is used by the SPI Flash Controller to update the HMAC-Key register corresponding to the received Counter Address with a new HMAC key calculated based on received input. This command must be issued once only on every power cycle event on the interface. This allows the HMAC key storage to be implemented using volatile memory. Status register busy indication is expected to indicate busy for double the amount of Read_Counter_Polling_Delay specified in SFDP table since this command performs two distinct HMAC-SHA-256 computations.

After the command is issued on the interface the Authentication Flash must ensure that the received transaction is error free. This includes checking following conditions:

- Payload size is correct. (including OP1 = 40 bytes)
- Counter Address falls within the range of supported counters.
- The Monotonic Counter corresponding to the requested Counter Address was previously initialized.
- Signature matches the HMAC-SHA-256 based signature computed based on received input parameters. This command performs two HMAC-SHA-256 operations.

If the received transaction is error free, the Authentication Flash successfully executes the command and posts “successful completion” in the Authentication Flash Status Register.

If the received transaction has errors, the Authentication Flash does not execute the transaction and posts the corresponding error in the Authentication Flash Status Register.

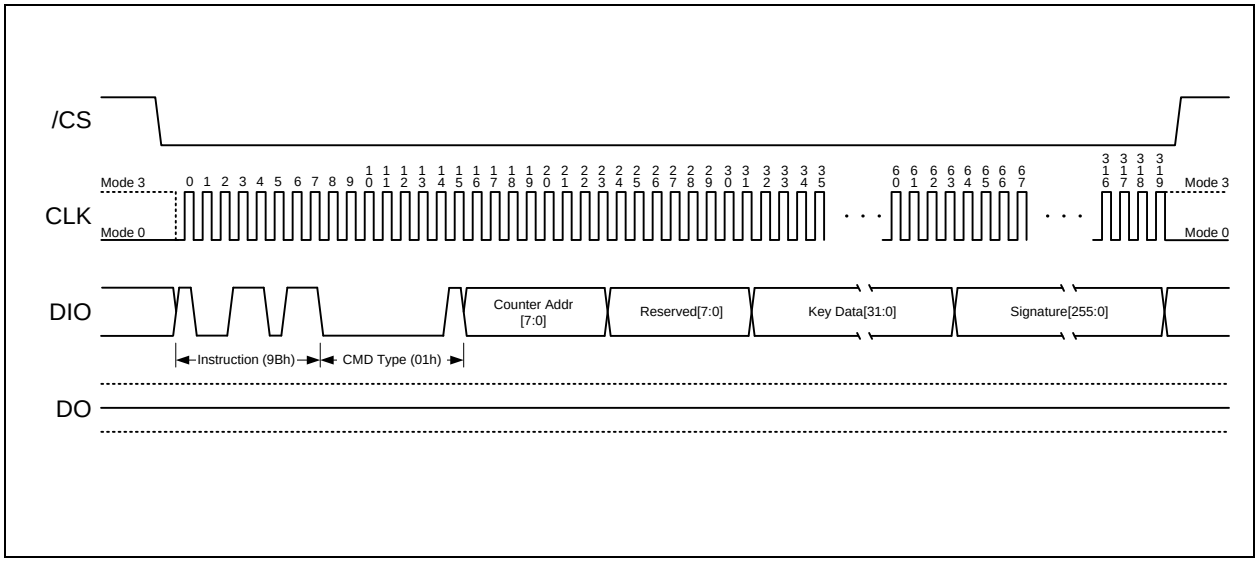


Figure 5. Update HMAC Key Register Instruction

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

6.3.3 Increment Monotonic Counter (9Bh + 02h)

This command is used by the SPI Flash Controller to increment the Monotonic Counter by 1 inside the Authentication Flash.

After the command is issued on the interface the Authentication Flash must ensure that the received transaction is error free. This includes checking following conditions:

- Payload size is correct. (including OP1 = 40 bytes)
- Counter Address falls within the range of supported counters.
- The Monotonic Counter corresponding to the requested Counter Address was previously initialized.
- The HMAC Key Register corresponding to the requested Counter Address was previously initialized.
- The requested Signature matches the HMAC-SHA-256 based signature computed based on received input parameters.
- The received Monotonic_Counter_Data matches the current value of the counter read from the SPI Flash.

If the received transaction is error free, the Authentication Flash successfully executes the command and posts “successful completion” in the Authentication Flash Status Register. The increment counter implementation should make sure that the counter increment operation is performed in a power glitch aware manner.

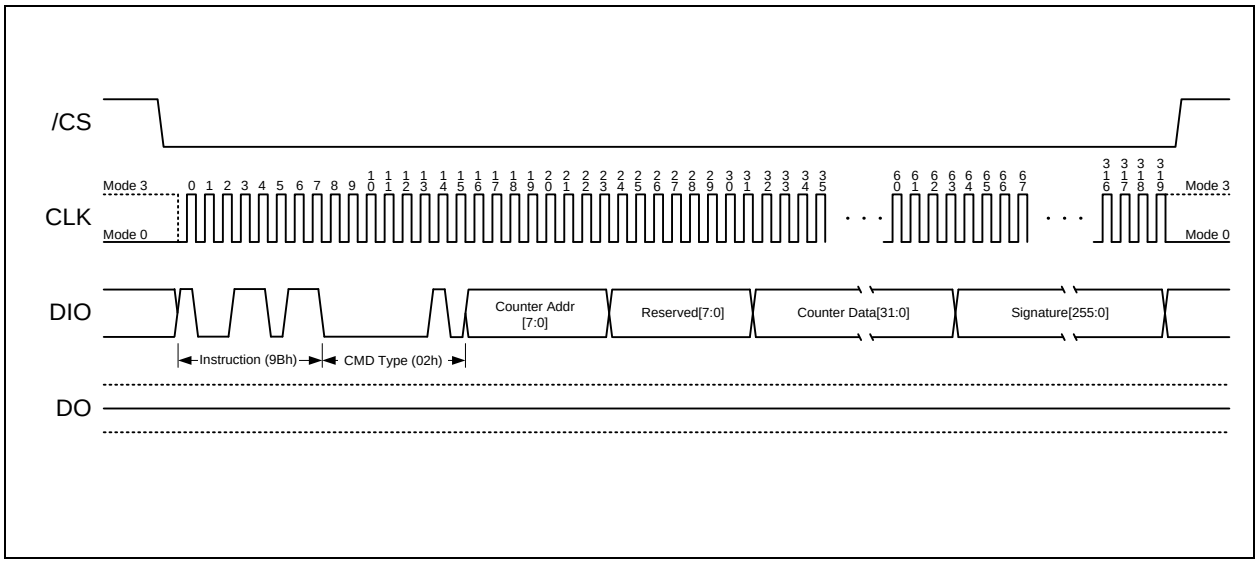


Figure 6. Increment Monotonic Counter Instruction

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

6.3.4 Request Monotonic Counter (9Bh + 03h)

This command is used by the SPI Flash Controller to request the Monotonic Counter value inside the Authentication Flash.

After the command is issued on the interface the Authentication Flash must ensure that the received transaction is error free. This includes checking following conditions:

- Payload size is correct. (including OP1 = 48 bytes)
- Counter Address falls within the range of supported counters.
- The Monotonic Counter corresponding to the requested Counter Address was previously initialized.
- The HMAC Key Register corresponding to the requested Counter Address was previously initialized.
- The requested Signature matches the HMAC-SHA-256 based signature computed based on received input parameters.

If the received transaction is error free, the Authentication Flash successfully executes the command and posts “successful completion” in the Authentication Flash Status Register. In response to this command, the SPI flash reads the Monotonic Counter addressed by counter address. It calculates HMAC-SHA-256 signatures the second time, based on following parameters.

- HMAC Message[127:0] = Tag [95:0], Counter_Data_Read[31:0]
- HMAC Key[255:0] = HMAC_Key_Register[Monotonic_Counter_Address][255:0]

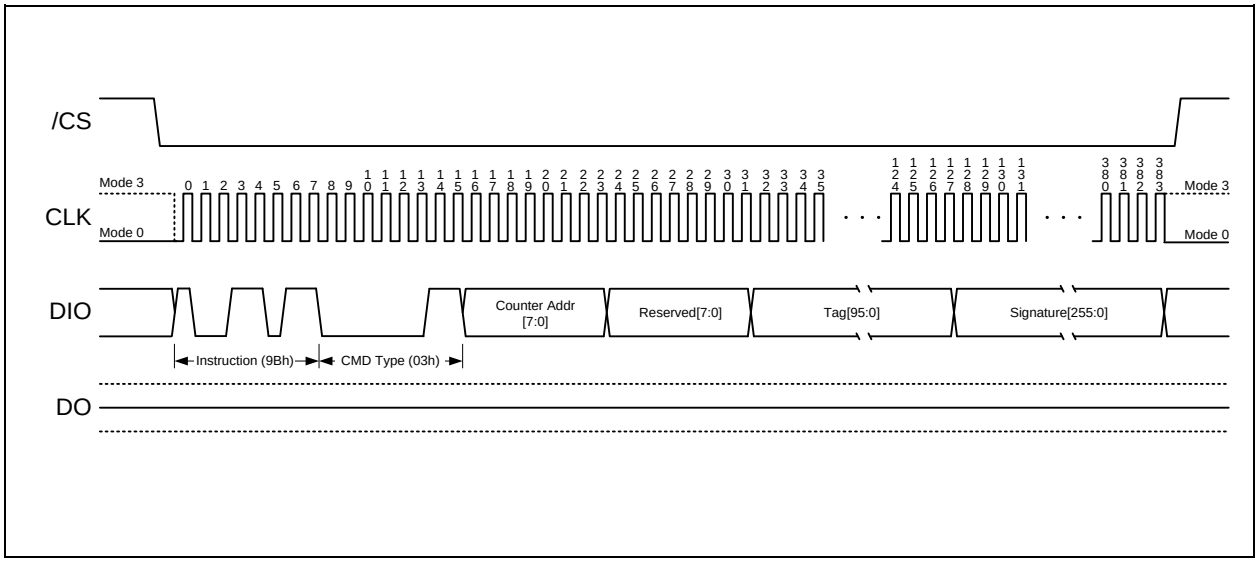


Figure 7. Request Monotonic Counter Instruction

6.3.5 Reserved Authentication Flash Device Commands (9Bh + 04h~FFh)

If the SPI Flash Controller issues any of the reserved command-types, the Authentication Flash must return Error status in the Authentication Flash Status Register. It asserts bit 2 to indicate that a reserved command-type was issued.

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

6.3.6 Read Authentication Flash Device Status / Data (96h)

This command is used by the SPI Flash Controller to read the Authentication Flash status from any previously issued OP1 command. In addition, if previous OP1 command is Request Monotonic Counter and if SPI Flash returns successful completion (BUSY=0) in the Authentication Flash Status Register, then it must also return valid values in the Tag, Monotonic_Counter_Data and Signature field. If there're other error flags, the values returned in Tag, Counter and Signature field are invalid. The controller may abort the read prematurely prior to completely reading the entire payload. This may occur when the controller wants to simply read the Authentication Flash status or when it observes an error being returned in the Authentication Flash status field. The controller may also continue reading past the defined payload size of 49 bytes. Since this is an error condition, the SPI Flash may return any data past the defined payload size. The controller must ignore the data.

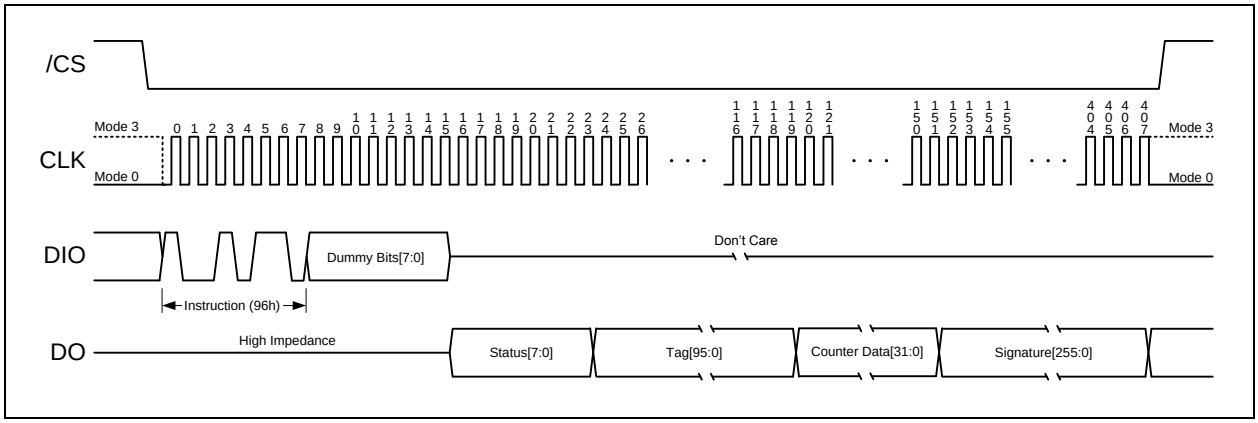


Figure 8a. Read Authentication Flash Data Instruction (BUSY=0)

When BUSY=1, from Byte-3 and beyond, the device will output the Authentication Flash Status[7:0] value continuously until /CS terminates the instruction. The device will not output Tag, CounterData & Signature fields when BUSY=1. Once BUSY becomes 0, another OP2 command must be issued to read out the correct Tag, CounterData & Signature fields.

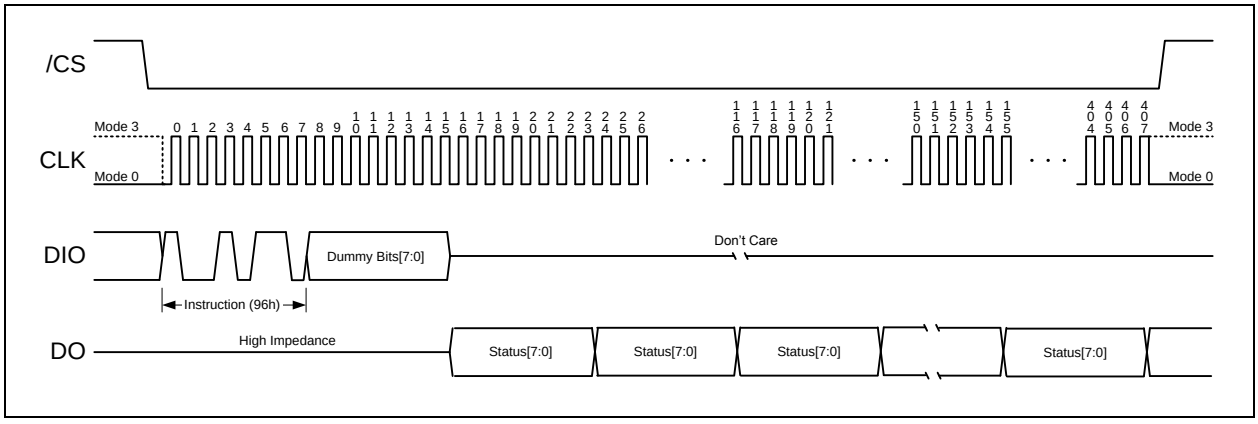


Figure 8b. Read Authentication Flash Data Instruction (BUSY=1)

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

6.3.7 Enable Reset (66h) and Reset Device (99h)

Because of the small package and the limitation on the number of pins, the Authentication Flash provide a software Reset instruction. Once the Reset instruction is accepted, any on-going internal operations will be terminated and the device will return to its default power-on state and lose all the current volatile settings, such as Volatile Status Register bits.

To avoid accidental reset, both instructions must be issued in sequence. Any other commands other than “Reset (99h)” after the “Enable Reset (66h)” command will disable the “Reset Enable” state. A new sequence of “Enable Reset (66h)” and “Reset (99h)” is needed to reset the device. Once the Reset command is accepted by the device, the device will take approximately tRST=30us to reset. During this period, no command will be accepted.

Data corruption may happen if there is an on-going when Reset command sequence is accepted by the device. It is recommended to check the BUSY bit Authentication Flash Register before issuing the Reset command sequence.

The “Enable Reset (66h)” and “Reset Device (99h)” commands only works on the authentication logic circuit. For the storage flash circuit reset, please refer to the datasheet of W25N01GV which can be found on Winbond web site http://www.winbond.com or www.spiflash.com.

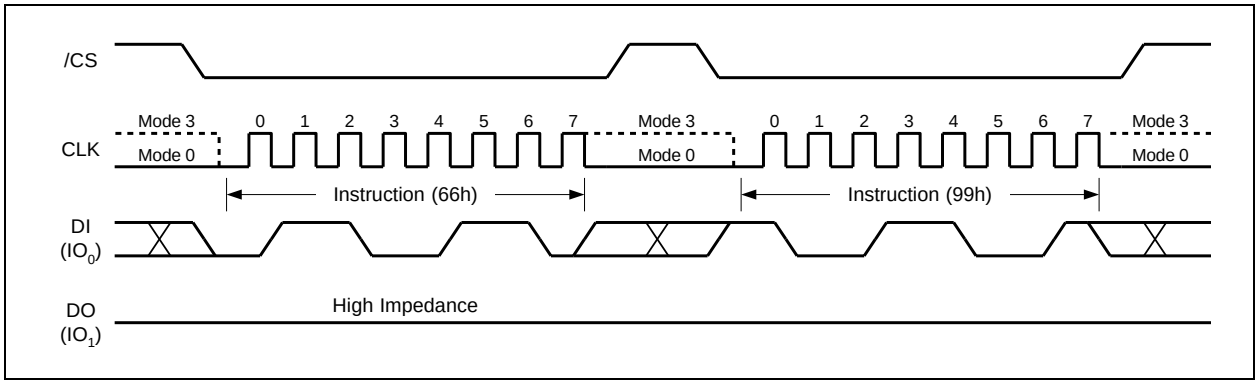


Figure 9. Enable Reset and Reset Instruction Sequence

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

7. ELECTRICAL CHARACTERISTICS(1)

7.1 Absolute Maximum Ratings (2)

PARAMETERS	SYMBOL	CONDITIONS	RANGE	UNIT
Supply Voltage	VCC		–0.6 to VCC+0.4	V
Voltage Applied to Any Pin	VIO	Relative to Ground	–0.6 to VCC+0.4	V
Transient Voltage on any Pin	VIOT	<20nS Transient Relative to Ground	–2.0V to VCC+2.0V	V
Storage Temperature	TSTG		–65 to +150	°C
Lead Temperature	TLEAD		See Note (3)	°C
Electrostatic Discharge Voltage	VESD	Human Body Model(4)	–2000 to +2000	V

Notes:

1. Specification for W74M01GV is preliminary. See preliminary designation at the end of this document.
2. This device has been designed and tested for the specified operation ranges. Proper operation outside of these levels is not guaranteed. Exposure to absolute maximum ratings may affect device reliability. Exposure beyond absolute maximum ratings may cause permanent damage.
3. Compliant with JEDEC Standard J-STD-20C for small body Sn-Pb or Pb-free (Green) assembly and the European directive on restrictions on hazardous substances (RoHS) 2002/95/EU.
4. JEDEC Std JESD22-A114A (C1=100pF, R1=1500 ohms, R2=500 ohms).

7.2 Operating Ranges

PARAMETER	SYMBOL	CONDITIONS	SPEC		UNIT
			MIN	MAX	
Supply Voltage	VCC	F_R = 80MHz	2.7	3.6	V
Ambient Temperature, Operating	TA	Industrial	–40	+85	°C

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

7.3 Power-Up Power-Down Timing and Requirements

PARAMETER	SYMBOL	SPEC		UNIT
		MIN	MAX	
VCC (min) to /CS Low	t_{VSL}(1)	50	500	µs
Time Delay Before Write Instruction	t_{PUW}(1)	5		ms
Write Inhibit Threshold Voltage	V_{WI}(1)	1.0	2.0	V

Note:

1. These parameters are characterized only.

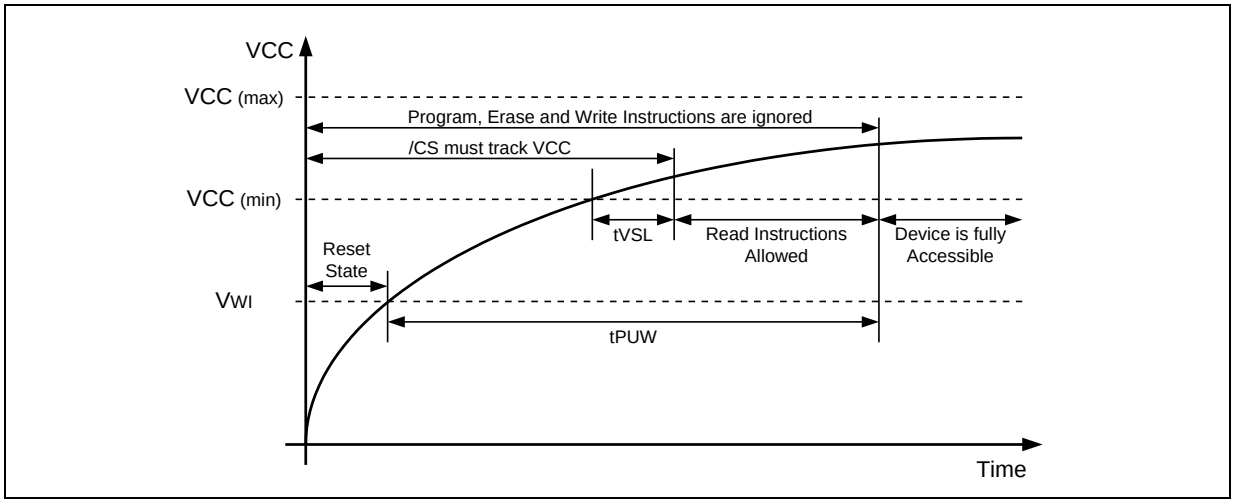


Figure 10a. Power-up Timing and Voltage Levels

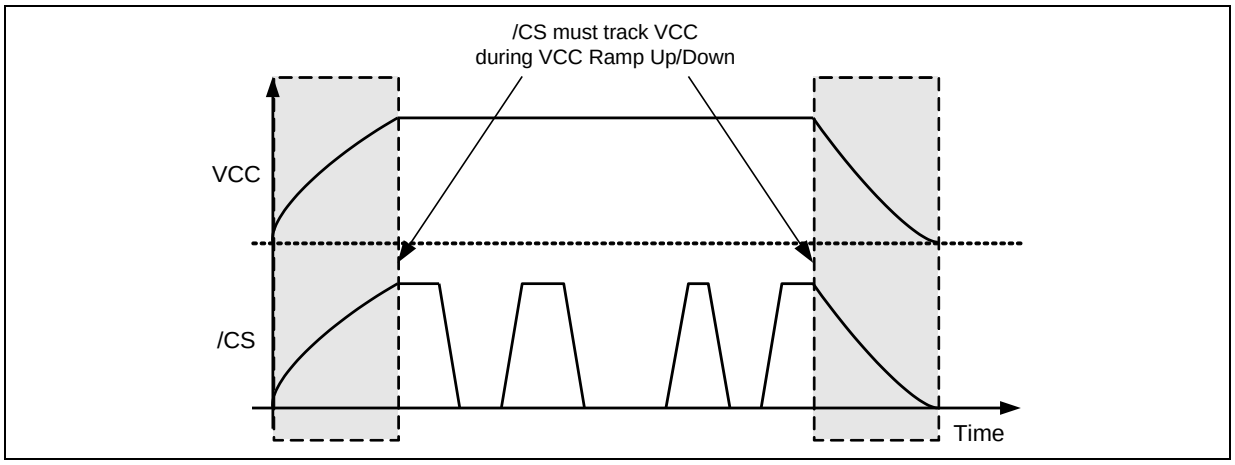


Figure 10b. Power-up, Power-Down Requirement

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

7.4 DC Electrical Characteristics(1)

PARAMETER	SYMBOL	CONDITIONS	SPEC			UNIT
			MIN	TYP	MAX	
Input Capacitance	C_{IN}(2)	V_{IN} = 0V			12	pF
Output Capacitance	C_{out}(2)	V_{OUT} = 0V			16	pF
Input Leakage	I_{LI}(2)				±4	µA
I/O Leakage	I_{LO}(2)				±4	µA
Standby Current	I_{CC1}(2)	/CS = VCC, VIN = GND or VCC		35	100	µA
Authentication Flash OP1 Write Only	I_{CC2}	/CS = VCC		15	20	mA
Authentication Flash OP2 Read Only	I_{CC3}	C = 0.1 VCC / 0.9 VCC			30	mA
Input Low Voltage	V_{IL}				VCC x 0.3	V
Input High Voltage	V_{IH}		VCC x 0.7		VCC+0.4	V
Output Low Voltage	V_{OL}	I_{OL} = 100 µA			0.2	V
Output High Voltage	V_{OH}	I_{OH} = –100 µA	VCC – 0.2			V

Notes:

1. Tested on sample basis and specified through design and characterization data. TA = 25° C, VCC = 3.0V.
2. The value includes SpiFlash and Authentication Flash.

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

7.5 AC Measurement Conditions

PARAMETER	SYMBOL	SPEC		UNIT
		MIN	MAX	
Load Capacitance	C_L		30	pF
Input Rise and Fall Times	T_R, T_F		5	ns
Input Pulse Voltages	V_{IN}	0.1 VCC to 0.9 VCC		V
Input Timing Reference Voltages	IN	0.3 VCC to 0.7 VCC		V
Output Timing Reference Voltages	OUT	0.5 VCC to 0.5 VCC		V

Note:

1. Output Hi-Z is defined as the point where data out is no longer driven.

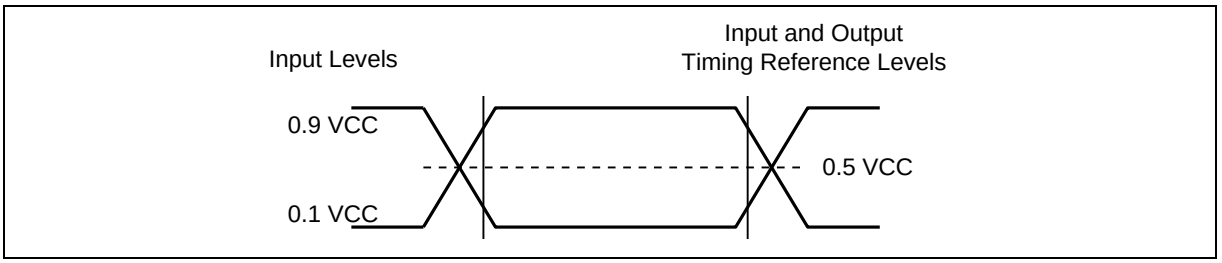


Figure 11. AC Measurement I/O Waveform

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

7.6 AC Electrical Characteristics(3,4)

DESCRIPTION	SYMBOL	ALT	SPEC			UNIT
			MIN	TYP	MAX	
Clock frequency for OP1/OP2	F_R	f_C	D.C.		80	MHz
Clock High, Low Time	t_{CLH}, t_{CLL}(1)		5			ns
Clock Rise Time peak to peak	t_{CLCH}(2)		0.1			V/ns
Clock Fall Time peak to peak	t_{CHCL}(2)		0.1			V/ns
/CS Active Setup Time relative to CLK	t_{SLCH}	t_{CSS}	5			ns
/CS Not Active Hold Time relative to CLK	t_{CHSL}		5			ns
Data In Setup Time	t_{DVCH}	t_{DSU}	2			ns
Data In Hold Time	t_{CHDX}	t_{DH}	5			ns
/CS Active Hold Time relative to CLK	t_{CHSH}		3			ns
/CS Not Active Setup Time relative to CLK	t_{SHCH}		3			ns
/CS Deselect Time	t_{SHSL}	t_{CSH}	50			ns
Output Disable Time / Output Disable Time	t_{SHQZ}	t_{DIS}			7 / 8.5	ns
Clock Low to Output Valid 2.7V-3.0V / 3.0V-3.6V	t_{CLQV1}	t_{V1}			7 / 6	ns
Clock Low to Output Valid for Authentication Flash OP2 command 2.7V-3.0V / 3.0V-3.6V	t_{CLQV2}	t_{V2}			8.5 / 7.5	ns
Output Hold Time	t_{CLQX}	t_{HO}	2			ns

Continued – next page

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

AC Electrical Characteristics (cont'd)

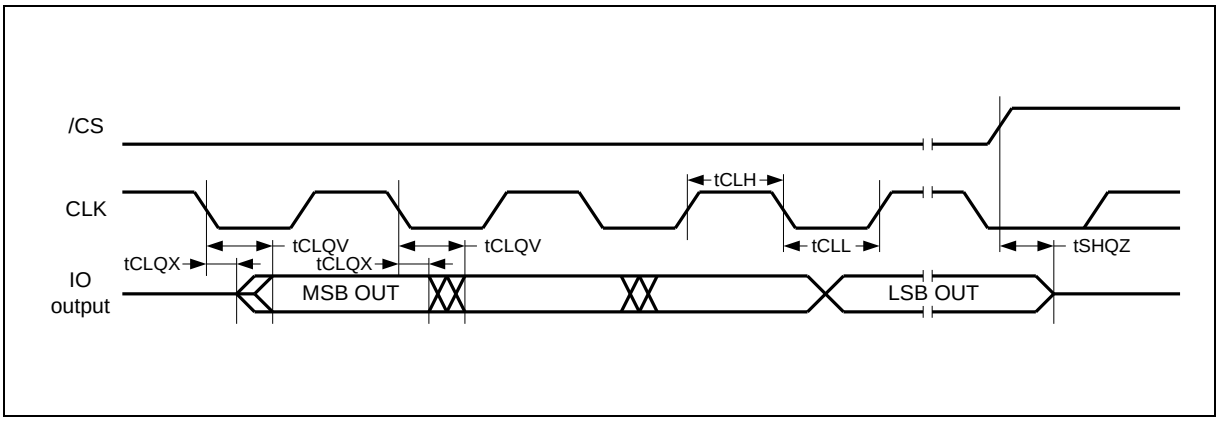
DESCRIPTION	SYMBOL	ALT	SPEC			UNIT
			MIN	TYP	MAX	
/CS High to Standby Mode	t_{RES1}(2)				3	µs
/CS High to next Instruction after Reset	t_{RST}(2)				30	µs
Write Root Key Register	t_{KEY}			170	250	µs
Update HMAC Key Register	t_{HMAC}			50	75	µs
Increment Monotonic Counter	t_{INC1}			80	200	µs
Increment Monotonic Counter (Counter Switching)	t_{INC2}			75	250	ms
Authentication Flash Request Monotonic Counter	t_{REQ}			80	120	µs

Notes:

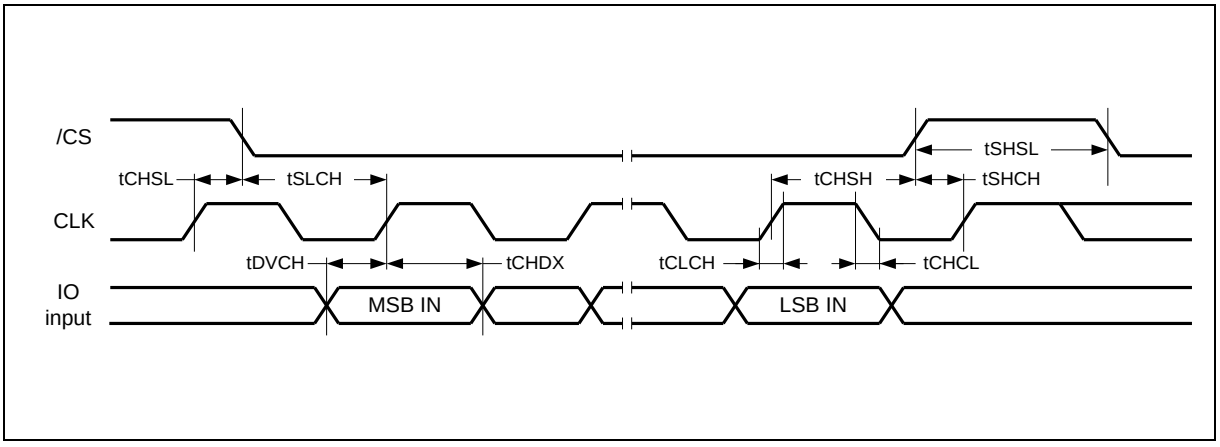
1. Clock high + Clock low must be less than or equal to 1/fC.
2. Value guaranteed by design and/or characterization, not 100% tested in production.
3. Tested on sample basis and specified through design and characterization data. TA = 25° C, VCC = 3.0V.

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

7.7 Serial Output Timing Diagram



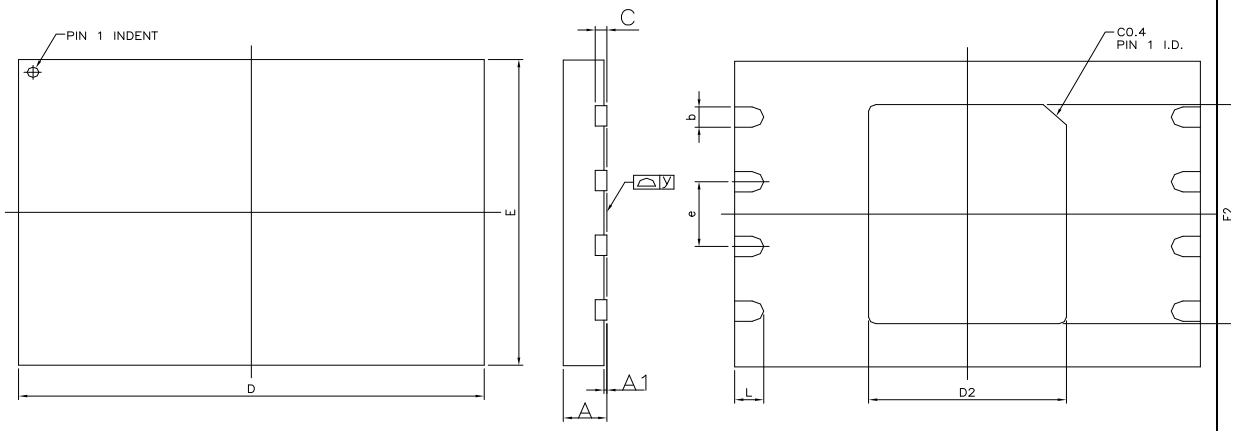
7.8 Serial Input Timing Diagram



深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

8. PACKAGE SPECIFICATIONS

8.1 8-Pad WSON 8x6-mm (Package Code ZE)



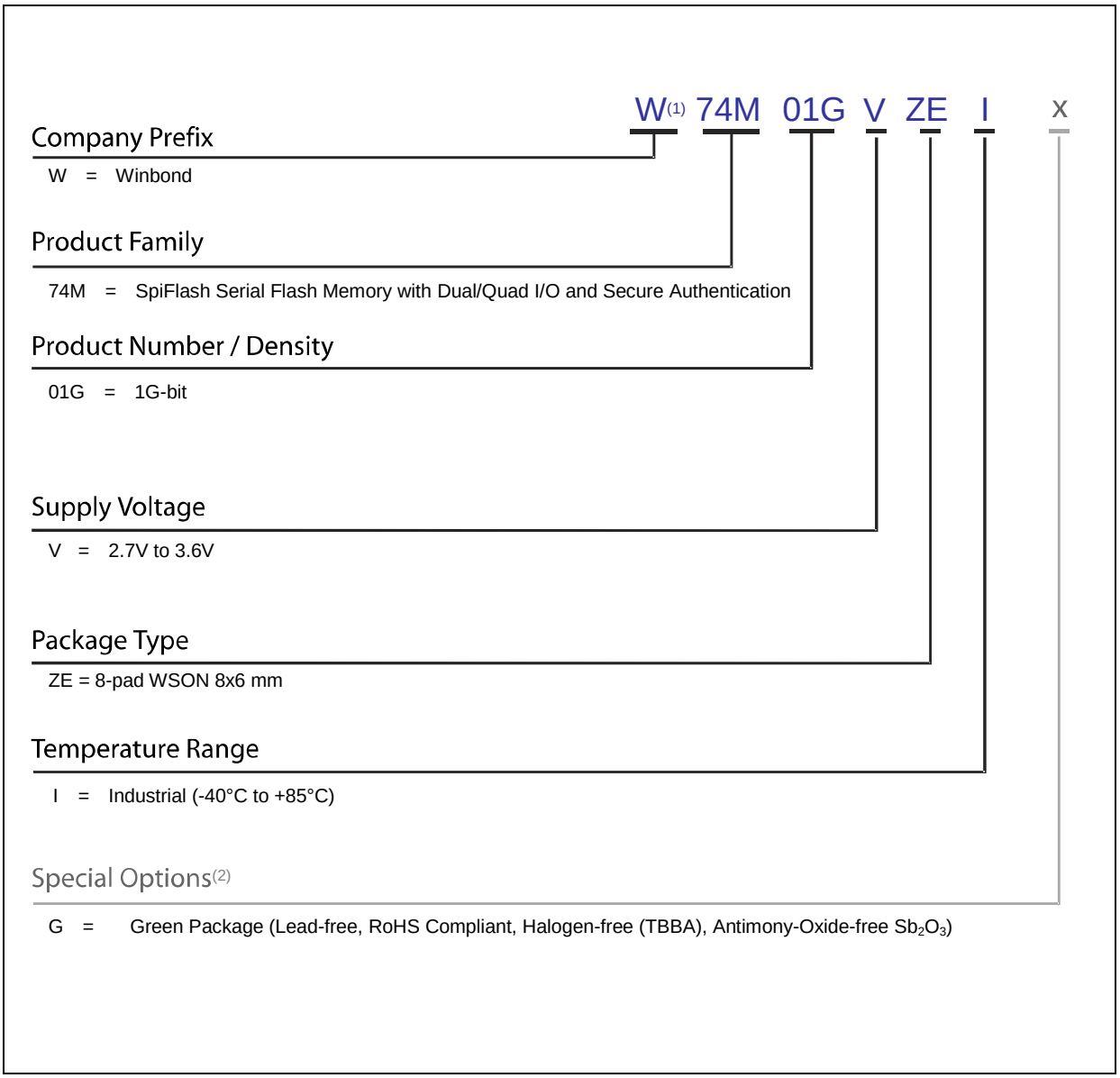
Symbol	Millimeters			Inches		
	Min	Nom	Max	Min	Nom	Max
A	0.70	0.75	0.80	0.028	0.030	0.031
A1	0.00	0.02	0.05	0.000	0.001	0.002
b	0.35	0.40	0.48	0.014	0.016	0.019
C	---	0.20 REF	---	---	0.008 REF	---
D	7.90	8.00	8.10	0.311	0.315	0.319
D2	3.35	3.40	3.45	0.132	0.134	0.136
E	5.90	6.00	6.10	0.232	0.236	0.240
E2	4.25	4.30	4.35	0.167	0.169	0.171
e	---	1.27	---	---	0.050	---
L	0.45	0.50	0.55	0.018	0.020	0.022
y	0.00	---	0.050	0.000	---	0.002

Note:

The metal pad area on the bottom center of the package is not connected to any internal electrical signals. It can be left floating or connected to the device ground (GND pin). Avoid placement of exposed PCB vias under the pad.

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

8.2 Ordering Information



Notes:

1. The “W” prefix is not included on the part marking.
2. Standard bulk shipments are in Tube (shape E). Please specify alternate packing method, such as Tape and Reel (shape T) or Tray (shape S), when placing orders.

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

8.3 Valid Part Numbers and Top Side Marking

The following table provides the valid part numbers for the W74M01GV. Please contact Winbond for specific availability of different package types. Winbond Authentication Flash use a 12-digit Product Number for ordering. However, due to limited space, the Top Side Marking on all packages uses an abbreviated 10-digit number.

PACKAGE TYPE	DENSITY	PRODUCT NUMBER	TOP SIDE MARKING
ZE WSON-8 8x6 mm	1G-bit	W74M01GVZEIG	74M01GVEIG

Note:

Contact Winbond for other package options.

9. GENERAL INSTRUCTIONS

Digit number for all Spi-Flash features, DC and AC parameters, and functions of this product, please refer to the datasheet of W25N01GV which can be found on Winbond web site http:// www.winbond.com or www.spiflash.com.

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com

10. REVISION HISTORY

VERSION	DATE	PAGE	DESCRIPTION
A	02/17/2017		New Create Preliminary

Preliminary Designation

The “Preliminary” designation on a *Winbond* datasheet indicates that the product is not fully characterized. The specifications are subject to change and are not guaranteed. *Winbond* or an authorized sales representative should be consulted for current information before using this product.

Trademarks

Winbond is a trademark of *Winbond Electronics Corporation.*
All other marks are the property of their respective owner.

Important Notice

Winbond products are not designed, intended, authorized or warranted for use as components in systems or equipment intended for surgical implantation, atomic energy control instruments, airplane or spaceship instruments, transportation instruments, traffic signal instruments, combustion control instruments, or for other applications intended to support or sustain life. Furthermore, *Winbond* products are not intended for applications wherein failure of *Winbond* products could result or lead to a situation wherein personal injury, death or severe property or environmental damage could occur. *Winbond* customers using or selling these products for use in such applications do so at their own risk and agree to fully indemnify *Winbond* for any damages resulting from such improper use or sales.

Information in this document is provided solely in connection with Winbond products. Winbond reserves the right to make changes, corrections, modifications or improvements to this document and the products and services described herein at any time, without notice.

Please note that all data and specifications are subject to change without notice.
All the trademarks of products and companies mentioned in this datasheet belong to their respective owners.

深圳市满度科技有限公司
Web:www.manduic.com
Tel:150-1290-5940
Email:sales@manduic.com