Serial Flash Hardening Product

External Architecture Specification (EAS)

Rev 0.7

Document Number: 328802-001EN

Legal Disclaimer

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by going to: http://www.intel.com/design/literature.htm.

Code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user.

Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

Table of Contents

TABLE OF FIGURES

Revision History:

Document Number	Revision Number	Description	Revision Date
328802-001EN	0.7	• Initial release.	March 2013

§

Acronyms and Definitions

Acronym or Term	Definition
RPMC	Replay Protected Monotonic Counter
EAS	External Architecture Spec, EAS has technical details on how to implement the PRD requirements
OEM	Original equipment manufacturer
SHA-256	SHA stands for Secure Hash Algorithm. SHA-256 refers to the SHA-2 family of algorithms with the digest size of 256 bits.
HMAC-SHA-256	In cryptography, **HMAC** (Hash-based Message Authentication Code) is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret 256 bit encryption key. As with any MAC, it may be used to simultaneously verify both the *data integrity* and the *authenticity* of a message. HMAC-SHA-256 uses SHA256
PCH	Platform controller hub is an integrated Southbridge connecting to the CPU

§

1 Introduction:

The Serial Flash is the persistent storage available on the motherboard of a PC platform. In PC platforms the Serial Flash contains CPU BIOS code. In addition it provides persistent storage support for a number of microcontrollers on the platform used for critical functions such as security and power management.

Serial Flash access control is enforced at a sector or a subsector granularity. A specific sector may be read only (write protected), or read/write (can be written to during run-time for normal functionality). The Flash read/write protection is performed by the Serial Flash Controller HW on the motherboard. In Intel platforms this function is integrated in the Peripheral Controller Hub (PCH) or South Bridge.

The security protections described above are necessary but not sufficient to meet advanced use cases of a PC. This document provides the requirements for an additional block called as Replay Protection Monotonic Counter. (RPMC) Replay Protection provides a building block towards providing additional security. This block requires modifications in both a Serial Flash device and Serial Flash Controller. The specification defines new commands for Replay Protected Monotonic Counter operations. A device that supports RPMC can support these new commands as defined in this specification.

§

2 Hardware Attack Vulnerabilities

The current definition of the Serial Flash does not offer any protection against HW attacks. HW attacks are defined as attacks where the attacker has physical access to Serial Flash. As a result the attacker is able to modify the flash content by de-soldering the part and reprogramming it or replacing it. Attacker is also able to capture information by probing it using a logic analyzer and replay it at a different time. Attacker is able to modify the flash content on the fly by inserting FPGA HW in the middle.

Such attacks are becoming relevant in sophisticated use cases where the attacker associates a value with persistent contents stored on the platform. As an example, the information stored on the platform provides a license to the user for access to services in the cloud. Or a cloud based service provider relies upon the goodness of the platform (secure boot, measured boot, license etc.) to ensure that the user and the platform meets the criteria associated with the availability of the service.

Such an attack can be detected by protecting monotonic counter values in the platform. This specification defines how monotonic counters can be protected using a new set of commands between the Serial Flash Controller and Serial Flash devices.

The overview of this capability is described below:

- Command to write 256 bit "Root Key".
  - The root key is stored inside the flash and is not readable from outside. This includes test modes. A non "0FF..FF" root key is programmed only one time during system manufacturing.
  - A 32 bit monotonic counter is associated with the root key. It is initialized to zero when a valid 256 bit write root key operation is performed regardless of the value of the root key. (ie "0FF..FFH or non "0FF..FFH)
- Authenticated commands/responses are commands/responses signed using the "HMAC Key". The signature is verified using HMAC-SHA-256.
  - The HMAC key is stored inside the flash and is not readable including via test modes.
- Authenticated "HMAC key update command" to derive a 256 bit HMAC key. The HMAC key is derived from the Root Key and Key data supplied during the command using HMAC-SHA-256. So this command performs two HMAC-SHA-256 operations. Once to derive the HMAC key and once to verify the signature.
- Authenticated commands to support following monotonic counter operations.
  - Increment counter
  - Read counter
- Support for a minimum of four counters with associated resources such as root key registers, HMAC key registers.

- No mechanism to circumvent Authenticated commands including via test modes. The Serial Flash device must meet following restrictions:
  - — Root key register erase operation can be performed using manufacturing test mode only without reading its value   At this point the root key register can be reprogrammed to fully test the part. The behavior of the associated counter during test mode erase root key is manufacturer dependent i.e. it can be initialized or it can retain its current value.
- No mechanism to circumvent Write/Erase commands for all standard sectors. The Serial Flash Controller write protects these sectors by preventing certain op-codes to be issued to the address range it wants to protect during run time. Serial Flash device must meet following restrictions:
  - — Write/Erase operation on sectors and subsectors can only be performed using standard op-codes as defined in the Serial Flash specification.

2.1 OP1/OP2 Command Definition: No Address Phase

Function	Opcode Phase 8 bits	Payload Phase Max 512 Bits		Comment
		Byte#	Field Description	
Command: Write Root Key Register	OP1	1	CmdType[7:0] = 00H	OP1 + Payload phase driven by host controller. A non 0FF..FFH Root Key Register is written only once.
		2	CounterAddr[7:0]	
		3	Reserved[7:0]	
		4-35	RootKey[255:0]	
		36-63	TruncatedSign[223:0]	
Command: Update HMAC Key Register	OP1	1	CmdType[7:0]= 01H	OP1 + Payload phase is Issued by host controller on every power up to initialize HMAC Key Register.
		2	CounterAddr[7:0]	
		3	Reserved[7:0]	
		4-7	KeyData[31:0]	
		8-39	Signature[255:0]	
Command: Increment Monotonic Counter	OP1	1	CmdType[7:0] = 02H	OP1 + Payload Phase is Issued by host controller during runtime to increment the counter.
		2	CounterAddr[7:0]	
		3	Reserved[7:0]	
		4-7	CounterData[31:0]	
		8-39	Signature[255:0]	
Command: Request Monotonic Counter	OP1	1	CmdType[7:0] = 03H	OP1 + Payload Phase is Issued by host controller during runtime to request counter data
		2	CounterAddr[7:0]	
		3	Reserved[7:0]	
		4-15	Tag[95:0]	

Function	Opcode Phase 8 bits	Payload Phase Max 512 Bits		Comment
		Byte#	Field Description	
		16-47	Signature[255:0]	
Command: Read Data	OP2	2	ExtendedStatus[7:0]	OP2 is issued by Host Controller generally after an OP1. Serial Flash device responds with the Payload phase to return Extended Status and counter data.
		3-14	Tag[95:0]	
		15-18	CounterData[31:0]	
		19-50	Signature[255:0]	
Reserved Commands	OP1	1	CmdType = 04H – 0FFH	These OP1 commands are reserved and cannot be used

All individual fields are Byte wide fields. For a multi-byte field, Most Significant Byte is issued first; Least Significant Byte is issued last. Within a Byte, Most Significant Bit is issued first; Least Significant Bit is issued last. CmdType is always the first byte issued after OP1 commands. OP2 delay is the same as Fast Read Command delay which is 8 dummy bits. OP1 and OP2 are defined for 1-0-1 mode only.

Byte #	0	1	2	3	4	5	6	…	..	..
Name	OP1	CmdType	Counter Address	As defined in the table above						
Name	OP2	8 Dummy clocks	Extended Status[7:0]	As defined in the table above						

After an OP1 command is received, the Serial Flash will indicate status busy indication using either the status register or extended status register[0] as defined below.

Extended Status Register Definition

Extended Status [7:0]	Applicable CmdType(s)	Description
00000000	-	Power On State (OP2 issued directly after power-up).
10000000	00, 01, 02, 03,	This status must be set on successful completion (no errors) of OP1 command.
0XXXXXX1	00, 01, 02, 03, 04-0FF	If Busy_Polling_Method bit in SFDP table is zero, then this bit must be set to 1, when device is busy executing OP1 command. It is reset to 0 when OP1 command execution is done. If Busy_Polling_Method bit in SFDP table is one, then this bit is ignored by the controller.
0XXXXX1X	00, 01	This bit is set only when the correct payload size is received. When cmdtype = 0, this error bit must be set

Extended Status [7:0]	Applicable CmdType(s)	Description
		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 montonic 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 and cmdtype = 02 or 03 and correct payload size is received
0XX1XXXX	02	This bit must be set on Counter Data Mismatch and cmdtype = 02 and correct payload size is received
0X1XXXXX	-	Fatal Error, e.g. program fail, no valid counter found after initialization. This can be set at the discretion of the flash vendor
Current value	-	Extended status register will naturally not be updated until first 8 bits of OP1 is received. However it is expected that if an error is found or extended status[0] needs to be set it is set within 8 clocks after OP1 is received.

Flash devices shall advertise RPMC capabilities via an additional SFDP table. The RPMC table's header fields are:

Header First DWord	
Bits	**Description**
7:0	Parameter ID LSB = 03H (Even parity, guaranteed to not overlap with any manufacturer's JEDEC ID)
15:8	Minor revision = 0
23:16	Major revision = 1
31:24	Parameter Length = 2
Header Second DWord	
Bits	**Description**
23:0	Parameter Table Pointer = < specified by flash device manufacturer>
31:24	Parameter ID MSB = 0FFH

Table 3 lists the contents of the RPMC parameter table.

First dword	
Bits	**Description**
31:28	Reserved: Must be 0FH

27:24	Update_Rate: Rate of Update = 5 * (2 ** Update_Rate) seconds
23:16	OP2 Opcode: Suggested Value 96H
15:8	OP1 Opcode: Suggested value 9BH
7:4	Num_Counter-1: Number of supported counters-1. Suggested value 3.
3	Reserved: Must be 1
2	Busy_Polling_Method : ‘0’: Poll for OP1 busy using OP2 Extended Status[0]. No OP1 Suspended State Support ‘1’: Poll for OP1 busy using Read Status (05H). Suspended State is supported
1	MC_Size ‘0’: Monotonic counter size is 32 bit ‘1’: Reserved
0	Flash_Hardening ‘0’: Flash Hardening is supported. '1' : Flash Hardening is not supported
Second dword	
31:24	Reserved : Must be FF
23:16	Write Counter Polling Long Delay Write + one HMAC Operation + Typical Sub Sector Erase Time. Suggested usage: Allows controller to conserve power to delay polling if the short delay is not sufficient for completion of the write operation Bit 7 : reserved Bits 6:5 : units (00=1ms, 01=16ms,10=128ms, 11= 1s) Bits4:0 : polling_long_delay_write_ counter
15:8	Write Counter Polling Short Delay Worst Case Write + one HMAC operation, No Erase. Suggested usage: Allows controller to conserve power by delaying polling Bit 7 : reserved Bits 6:5 : units (00=1us, 01=16us, 10=128us, 11=1ms) Bits4:0 : polling_short_delay_write_ counter
7:0	Read Counter Polling Delay Typical case to calculate HMAC two times. Suggested usage: Allows controller to conserve power by delaying polling for read monotonic counter or update HMAC register commands. Bit 7 : reserved Bits 6:5 : units (00=1us, 01=16us, 10=128us, 11=1ms) Bits4:0 : polling delay_read counter

2.2 Operations Allowed / Disallowed During RPMC Operation

A Reset command (or a HW reset) will cause the part to get fully reset. All volatile memory based resources will be cleared. Update HMAC Key register command has to be explicitly reissued after a reset. While in the deep power down state OP1, OP2 commands are ignored until the part comes out of deep power down state.

WEL (Write Enable Latch) state does not affect the OP1 command execution inside the Serial Flash.

Suspend operation can be used to execute high-priority reads from the flash device while a long-latency operation is underway. OP1 is not allowed to be issued during Suspended State of the Serial Flash device. OP2 is allowed during Suspended State of the Serial Flash device; however the data returned in response to OP2 during Suspended State cannot be relied upon.

In the table below, OP1 state is defined as the time starting with a transaction with OP1 op-code sent to the device and ending when the device clears both the status busy bit and the extended status busy bit. During OP1 state if a suspend transaction is received, the Serial Flash part may optionally enter OP1 suspended state as described in Option 1 in the table below or remain in OP1 state as described in Option 2 in the table below. OP1 suspended state may be the same as suspended state. It starts when the device sets the program suspend status done bit after receiving a program suspend op-code (typically 30 us after receiving the suspend transaction). The controller is required to wait till the part enters the OP1 suspended state before it issues a subsequent flash transaction. With Option 2 the Serial flash part must be capable of supporting concurrent operation of OP1 and subsequent flash transactions.

Operation	**Option 1 (OP1 Suspended State Supported)**		**Option 2 (No OP1 suspended state)**
	OP1 state	**OP1 Suspended State**	**OP1 State**
Suspend	Yes -> OP1 Suspended State	No	Ignored
Resume	No	Yes -> OP1 state	Ignored
All reads except read status	No	Yes	Yes
All writes/erases	No	No	Yes
OP1	No	No	No
Write status	No	No	Yes
OP2	Yes ->OP1 busy state (when extended status busy is 1) ->OP1 done state (when extended status busy is 0)	Yes (Data returned is not reliable)	Yes->OP1 busy state (when extended status busy is 1) ->OP1 done state (when extended status busy is 0)
Read status	Yes -> OP1 busy state (when status busy is 1) ->OP1 partially done state (when status busy is 0)	Yes	Yes. Will indicate the busy state associated with the subsequent transaction issued to the Serial Flash.

Figure 1: Block Diagram

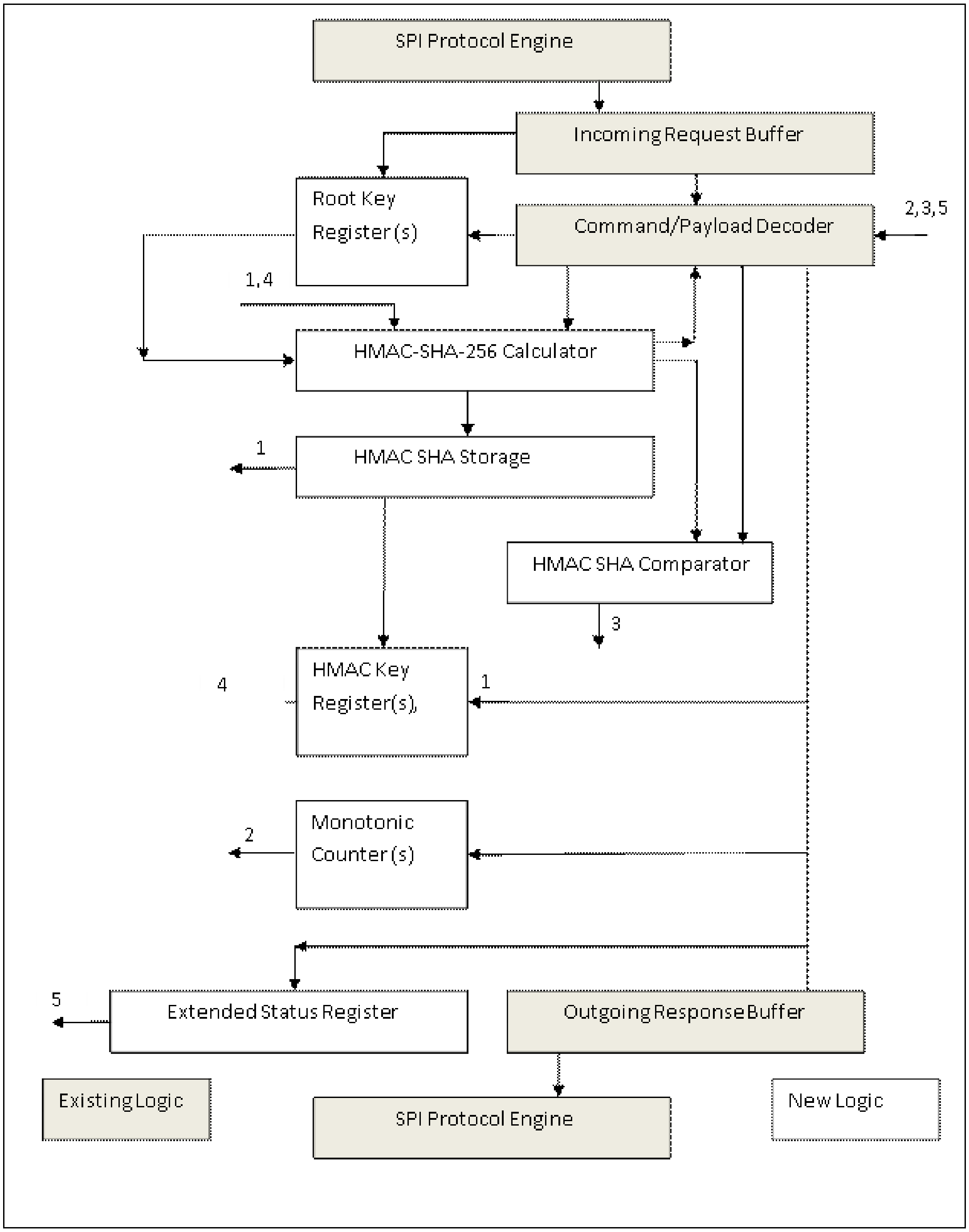
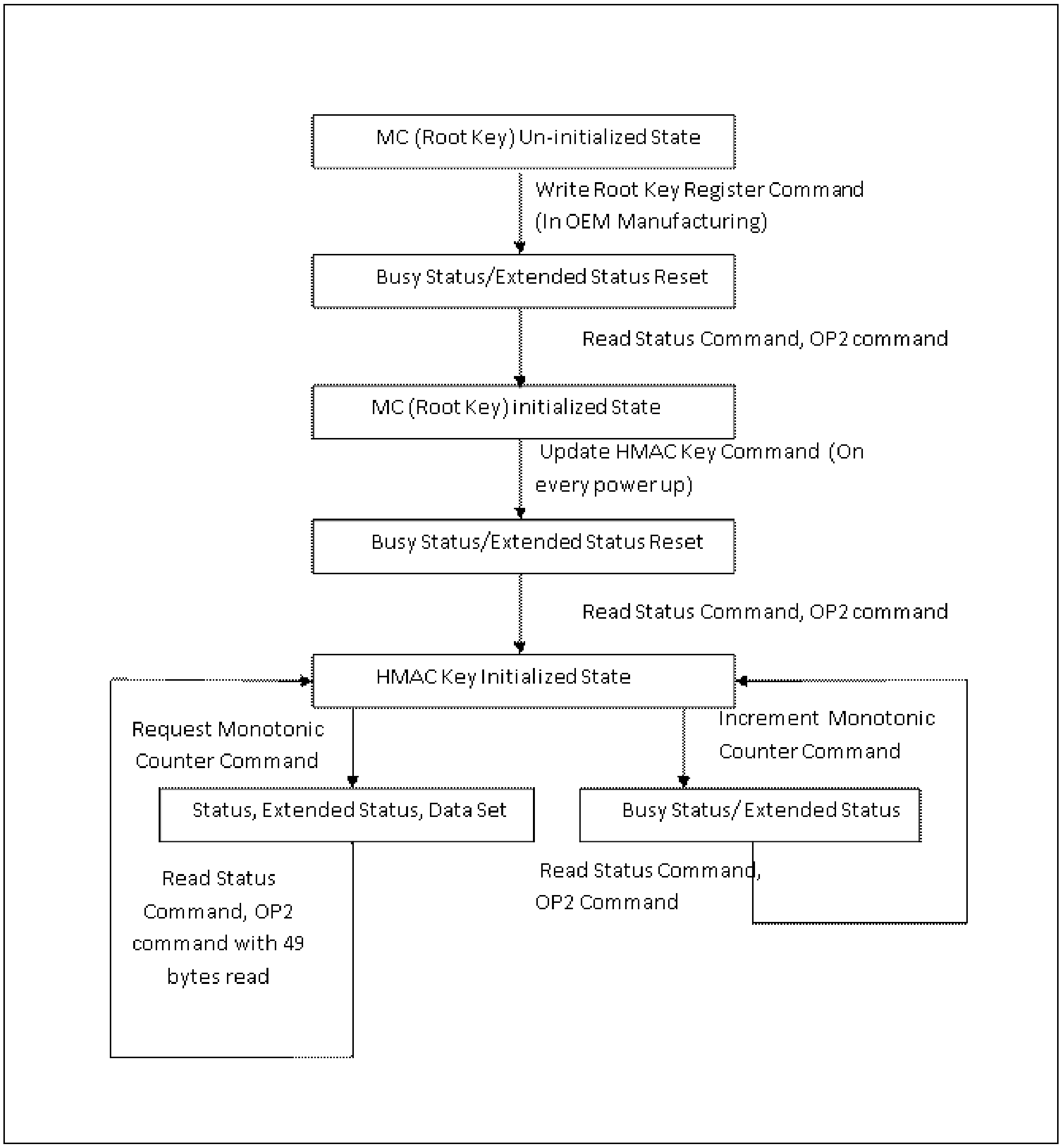


Figure 2: Example Command Flow Overview


MC (Root Key) Un-initialized State
Write Root Key Register Command
(In OEM Manufacturing)
Busy Status/Extended Status Reset
Read Status Command, OP2 command
MC (Root Key) initialized State
Update HMAC Key Command (On
every power up)
Busy Status/Extended Status Reset
Read Status Command, OP2 command
HMAC Key Initialized State
Request Monotonic
Counter Command
Increment Monotonic
Counter Command
Status, Extended Status, Data Set
Busy Status/ Extended Status
Read Status
Command, OP2
command with 49
bytes read
Read Status Command,
OP2 Command

(Root Key) Initialized State is reached only when a non “0FF…FF” Root Key is received during Write Root Key Register Command.

This section describes the typical command flow for individual counter. The subsequent sections describe the detailed operation after each command is received.

2.3 Command: Write Root Key Register

This command is used by the Serial Flash 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 Serial Flash Controller and Serial Flash are powered together for the first time.

Byte #	0	1	2	3	4	5	6	7	…	34	35
Name	Opcode = OP1	Cmd Type = 00	Counter Addr [7:0]	Rsvd	Root Key[255:0]						
In_Message	511:504	503:496	495:488	487:480	479:224						

Byte #	36	37	38	39	…	62	63
Name	TruncatedSignature[223:0]						
In_Message	223:0						

After the command is issued on the interface the Serial Flash device 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[Counter_Address] = 0FFH]
- Truncated signature field is the same as least significant 224 bits of HMAC-SHA-256 based signature computed based on received input parameters:
  - HMAC message[31:0] = (OpCode[7:0], CmdType[7:0], CounterAddr[7:0], Reserved[7:0])
  - HMAC Key[255:0] = Root_Key[255:0]

If the received transaction is error free Serial Flash device successfully executes the command and posts "successful completion" extended status. 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[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[Counter_Address] is not affected. Instead only the corresponding Monotonic Counter is initialized to 0 if previously uninitialized. This state is tracked as a separate state using MC_Init_State[Counter_Address]. This state is used to leave the monotonic counters at the current value when a subsequent error free Root Key Register Write operation is received. (Both 256'HFF..FF and non 256'HFF..FF)

The various steps when root key register operation is received is as follows. The order of these steps is important in order to ensure a power glitch aware design.

- MC_Init_State is checked. If MC_Init_State is uninitialized, the monotonic counter is initialized and MC_Init_State[Counter_Address] is set to Initialized State.
- Root Key = 256'HFF.FF is checked. If Root Key != 256'HFF..FF then permanent root key is written to the root key register and Root_Key_Reg_Init_State[Counter_address] is set to Initialized State.
- HMAC_Key_Reg_Init_State[Counter_Address] is reset to uninitialized state.

If the received transaction has errors the Serial Flash does not execute the transaction and posts the corresponding error in extended status.

Extended Status [7:0]	**Applicable CmdType(s)**	**Description**
10000000	00	Successful completion
0XXXXXX1	00	If Busy_Polling_Method bit in SFDP table is zero, then this bit must be set to 1, when device is busy executing command. It is reset to 0 when OP1 command execution is done. If Busy_Polling_Method bit in SFDP table is one, then this bit is ignored by the controller.
0XXXXX1X	00	This bit is only set when correct payload size is received. It is set on Root Key Register Overwrite or Counter Address is out of range or when there is a truncated signature mismatch error
0XXXX1XX	00	This bit is set when incorrect payload size is received.

2.4 Command: Update HMAC Key Register

This command is used by the Serial 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 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.

Byte #	0	1	2	3	4	5	6	7
Name	Opcode = OP1	CmdType = 01	Counter Address	Rsvd	Key Data			
In_Message	511:504	503:496	495:488	487:480	479:448			

Byte #	8	9	10	11	12	13	14	…	38	39
Name	Signature[255:0]									
In_Message	447:192									

After the command is issued on the interface the Serial Flash device 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.
  - — HMAC-SHA-256 Operation 1 Output = HMAC_Storage[255:0]
    - — HMAC Message[31:0] = KeyData[31:0]
    - — HMAC Key[255:0] = Root_Key_Register[CounterAddr][255:0]
  - — HMAC-SHA-256 Operation 2 Output = HMAC-SHA-256 based signature[255:0]
    - — HMAC message[63:0] = (OpCode[7:0], CmdType[7:0].CounterAddr[7:0].Reserved[7:0], KeyData[31:0])
    - — HMAC Key[255:0] = HMAC_Storage[255:0]

If the received transaction is error free Serial Flash device successfully executes the command and posts "successful completion" extended status.

If the received transaction has errors the Serial Flash does not execute the transaction and posts the corresponding error in extended status.

Expected Extended Status [7:0] results

Extended Status [7:0]	**Applicable CmdType(s)**	**Description**
10000000	01	This status must be set on successful completion (no errors) of OP1 command.
0XXXXXX1	01	If Busy_Polling_Method bit in SFDP table is zero, then this bit must be set to 1, when device is busy executing OP1 command. It is reset to 0 when OP1 command execution is done. If Busy_Polling_Method bit in SFDP table is one, then this bit is ignored by the controller.
0XXXXX1X	01	This bit is set only when the correct payload size is received. This bit is set when the corresponding monotonic counter is uninitialized
0XXXX1XX	01	This bit must be set on Signature Mismatch, Counter Address out of range when correct payload size is received; or incorrect payload size is received.

2.5 Command: Increment Monotonic Counter

This command is used by the Serial Flash Controller to increment the Monotonic counter by 1 inside the Serial Flash Device.

Byte #	0	1	2	3	4	5	6	7
Name	Opcode = OP1	CmdType = 02	Counter Addr	Rsvd	Counter Data			
In_Message	511:504	503:496	495:488	487:480	479:448			

Byte #	8	9	10	11	12	13	...	37	38	39
Name	Signature									
InMessage	447:192									

After the command is issued on the interface the Serial Flash device 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.
  - HMAC Message[63:0] = (OpCode[7:0], CmdType[7:0]. CounterAddr[7:0]. Reserved[7:0], CounterData[31:0])
  - HMAC Key[255:0] = HMAC_Key_Register[Counter_Addreess][255:0]
- The received Counter Data matches the current value of the counter read from the Serial Flash.

If the received transaction is error free Serial Flash device successfully executes the command and posts "successful completion" extended status. The increment counter implementation should make sure that the counter increment operation is performed in a Power glitch aware manner. Due to 100,000 cycle erase limit, a 32 bit counter may require larger than 32 bit resources. An example implementation is described in section 2.10.

If the received transaction has errors the Serial Flash does not execute the transaction and posts the corresponding error in extended status.

Expected Extended Status [7:0] results

Extended Status [7:0]	Applicable CmdType(s)	Description
10000000	02	This status must be set on successful completion (no errors) of OP1 command.
0XXXXXX1	02	If Busy_Polling_Method bit in SFDP table is zero, then this bit must be set to 1, when device is busy executing OP1 command. It is reset to 0 when OP1 command execution is done. If Busy_Polling_Method bit in SFDP table is one, then this bit is ignored by the controller.
0XXXX1XX	02	This bit must be set on Signature Mismatch, Counter Address out of range when correct payload size is received; or incorrect payload size is received.
0XXX1XXX	02	This bit is set only when the correct payload size is received. This bit must be set on HMAC Key Register (or Monotonic Counter) is uninitialized on previous OP1 command.
0XX1XXXX	02	This bit is set only when the correct payload size is received. The bit must be set when the received counter data filed does not match the actual counter value read from the Serial Flash device.

2.6 Command: Request Monotonic Counter

This command is used by the Serial Flash Controller to request the Monotonic counter value inside the Serial Flash Device.

Byte #	0	1	2	3	4	5	6	..	..	13	14	15
Name	Opcode = OP1	CmdType = 03	Counter Address	Rsvd	Tag[95:0]							
In_Message	511:504	503:496	495:488	487:480	479:384							

Byte #	16	17	18	19	20	21	…	45	46	47
Name	Signature[255:0]									
In_Message	383:128									

After the command is issued on the interface the Serial Flash device 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.
  - — HMAC Message[127:0] = (OpCode[7:0], CmdType[7:0]. CounterAddr[7:0]. Reserved[7:0], Tag[95:0])
  - — HMAC Key[255:0] = HMAC_Key_Register[Counter_Addreess][255:0]

If the received transaction is error free Serial Flash device successfully executes the command and posts "successful completion" extended status. In response to this command, the Serial 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[Counter_Address][255:0]

It loads the outgoing response buffer[383:0] with the resulting signature

- Outgoing response buffer[383: 288] = Tag[95:0].
- Outgoing response buffer[287:256] = Counter_Data[31:0]
- Outgoing response buffer[255:0] = Signature[255:0])

If the received transaction has errors the Serial Flash does not execute the transaction and posts the corresponding error in extended status.

Expected Extended Status [7:0] results

Extended Status [7:0]	Applicable CmdType(s)	Description
10000000	03	This status must be set on successful completion (no errors) of OP1 command.
0XXXXXX1	03	If Busy_Polling_Method bit in SFDP table is zero, then this bit must be set to 1, when device is busy executing OP1 command. It is reset to 0 when OP1 command execution is done. If Busy_Polling_Method bit in SFDP table is one, then this bit is ignored by the controller.
0XXXX1XX	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.

Extended Status [7:0]	Applicable CmdType(s)	Description
0XXX1XXX	03	This bit is set only when the correct payload size is received. This bit must be set on HMAC Key Register (or Monotonic Counter) is uninitialized on previous OP1 command.

2.7 Command: Reserved Command-type

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

Expected Extended Status [7:0] results

Extended Status [7:0]	Applicable CmdType(s)	Description
0XXXX1XX	04-0FF	Cmd-type out of range

2.8 Command: Read Data

This command is used by the Serial Flash Controller to read extended status from any previously issued OP1 command. In addition if previous OP1 command is Request Monotonic Counter and if Serial Flash returns successful completion extended status then it must also return valid values in the Tag, Counter Data and Signature field. Otherwise 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 extended status or when is observes an error being returned in the extended status field. The controller may also continue reading past the defined payload size of 49 bytes. Since this is an error condition, the Serial Flash may return any data past the defined payload size. The controller must ignore the data.

Byte #	0	1	2	3	4	5	..	..	12	13	14
Name	Opcode [7:0 = OP2	8 Dummy Clocks	Extended Status [7:0]	Tag[95:0]							
Out_message			391:384	383:288							

Byte #	15	16	17	18	19	20	21	..	..	48	49	50
Name	CounterReadData				Signature							
Out_Message	287:256				255:0							

Byte #	51	52	53									
Name	Don't Care											
Out_Message	Ignored by the controller											

Extended Status Register Definition

Extended Status [7:0]	**Applicable CmdType(s)**	**Description**
00000000	-	Power On State (OP2 issued directly after power-up).
10000000	00, 01, 02, 03,	This status must be set on successful completion (no errors) of OP1 command.
0XXXXXX1	00, 01, 02, 03, 04-0FF	If Busy_Polling_Method bit in SFDP table is zero, then this bit must be set to 1, when device is busy executing OP1 command. It is reset to 0 when OP1 command execution is done. If Busy_Polling_Method bit in SFDP table is one, then this bit is ignored by the controller.
0XXXXX1X	00, 01	This bit is set only when the correct payload size is received. When cmdtype = 0, this error bit must be set on Root Key Register Overwrite or Counter Address out of range or Truncated Signature mis-match error. For remaining cmdtype = 1 this bit is set when the corresponding monotonic counter is uninitialized
0XXXX1XX	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 Root Key register) uninitialized on previous OP1 command when correct payload size is received
0XX1XXXX	02,	This bit must be set on 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. This can be set at the discretion of the flash vendor

Extended Status [7:0]	Applicable CmdType(s)	Description
Current value	-	Extended status register will naturally not be updated until first 8 bits of OP1 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.

§

3 References

The sections below contain various references.

3.1 Cryptographic Algorithms

As a reference please consult the official definition on NIST website.

SHA-256: Secure Hash Algorithm

http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf

HMAC-SHA-256: Hash Based Message Authentication Code

http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf

3.2 SFDP

As a reference please consult the official definition on JEDEC website and search for the latest revision of JESD216

http://www.jedec.org/standards-documents/results/field_25%3A%22JESD216%22

§