DS28E38 Security User Guide

UG6468; Rev 0; 9/17

Abstract

This security user guide contains detailed information about the device function commands of the DS28E38. It must be used in conjunction with its corresponding data sheet, which contains pin descriptions, feature overviews, and electrical specifications.

DS28E38EVKIT Developer Software

To download the full **DS28E38EVKIT Developer Software**:

1. Log in to your **MyMaxim** account, or create a new profile.
2. Click the button below to automatically download the software.

   Note: *In order for the download to start via the below button, you must first be logged in.*

   Download Software >

Table of Contents

List of Figures

List of Tables

General Information

The DS28E38 is an ECDSA public-key-based secure authenticator that incorporates Maxim's patented ChipDNA™ feature, a physically unclonable function (PUF) to provide a cost-effective solution with the ultimate protection against security attacks. This security guide describes the command sequences to use ChipDNA with the cryptographically secure device data, and to operate the ECDSA engine, the decrement-only counter, and the unique 64-bit ROM identification number (ROM ID). After a 1-Wire® Reset/Presence cycle and ROM function command sequence is successful, a DS28E38 is ready to accept the device function command sequence. Common to all device function commands is a command start issued first followed by a length byte, the device function command, and the parameter byte(s). The master receives a 16-bit CRC as confirmation of the device function command sequence to verify that it was received properly. Then the release byte can be issued followed by a delay with strong pullup (i.e., a low impedance bypass to supply high current demands during command processing). When the delay is complete, the master transmits a dummy byte and receives the length byte and result byte from DS28E38. Depending on the length byte received, subsequent result data may or may not be sent after the result byte. Finally, the master receives another 16-bit CRC as confirmation of the data DS28E38 sent after the dummy byte.

Usage Example—Feature (User Memory) Authentication with ECDSA

Setup

- On power-up, populate the ROM ID serial number with a Skip ROM command followed by a Read Status command
- Perform ROM command to read ROM ID
- Perform Generate ECC-256 Key Pair with Lock (write protection) enabled
- Perform Read Memory to read the Public Key
- Perform Write Memory to write certificate to user pages to authenticate device public key
- Perform Set Protection to set WP on certificate pages
- Perform Write Memory to set features to user page(s)
- Perform Set Protection to set WP on feature page(s)

Usage (Read Feature)

- On power-up, populate the ROM ID serial number with a Skip ROM command followed by a Read Status command
- Perform ROM command to read ROM ID
- Perform Read Memory for device Public Key
- Perform Read Memory on user pages with device certificate, master verifies certificate for device Public Key
- Perform Read Memory on feature page(s)
- Perform Compute and Read Page Authentication on feature page(s)
- Master verifies the signature with the device Public Key

Memory Resources

A secured 2Kb EEPROM array is configured to provide six of eight pages of programmable memory as shown in Table 1. Any of these first six of eight pages can be used for user memory or certificates. Optionally, page 3 can be used for the decrement counter. Pages 4 and 5 are used for public key X/Y, and share the same page protection. Setting one page automatically sets the other. Pages 4 and 5 also can optionally be used for user memory or certificates if the private key is set to a fixed value, so the public key does not need to be stored in the device. Two of the eight pages are reserved. In other words, one of these eight pages is reserved for an encrypted private key and the second of the eight pages is reserved for control registers. Optionally, this private key can be configured to use the PUF directly and page 6 contents is ignored. Lastly, each page of memory is 32 bytes.

Table 1. User Memory Map with Default Protections (32-Byte Pages)

PAGE	TYPE	DEFAULT PROTECTION	OPTIONAL PROTECTION
0–2	User/Certs	—	RP, WP, EM
3	User/Certs/Decrement Counter	—	RP, WP, EM, DC
4, 5	Pub Key X/Y (or User/Certs)	—	RP, WP, EM
6	Private Key	RP	WP (PF*)

**All protection is writable one time and permanent, except for PF. This indicates that the PUF is used as the device private key instead of the contents of page 6.*

PROTECTIONS TYPES	
PROTECTION	**DESCRIPTION**
RP	Read protect
WP	Write protect
EM	EPROM emulation (only set bits to 0)
DC	17-bit decrement counter enabled on page 3
PF	Private key is designated as the PUF (can be changed if WP is not also set)

64-Bit ROM ID

Each DS28E38 contains a unique ROM ID that is 64 bits long. The ROM ID is a fundamental input parameter for most cryptographic operations. The first 8 bits are a 1-Wire family code. The next 48 bits are a unique serial number. The last 8 bits are a cyclic redundancy check (CRC) of the first 56 bits. See Figure 1 for details. The 1-Wire CRC is generated using a polynomial generator consisting of a shift register and XOR gates. The polynomial is $X^8 + X^5 + X^4 + 1$. Additional information about the 8-bit 1-Wire CRC is available in Maxim Application Note 27.

On power-up, the 48-bit serial number of the ROM ID is zero. The family code and CRC-8, however, are correct. After any device level command, the 48-bit serial number is populated.

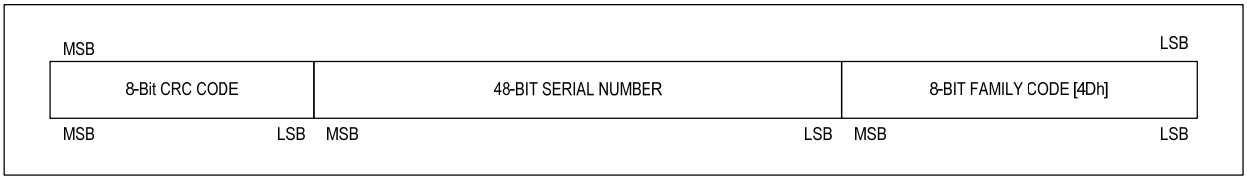

Figure 1. 64-bit ROM ID.

Device Function Commands

After a 1-Wire Reset/Presence cycle and ROM function command sequence is successful, a device function command can be accepted. The device function commands, in general, follow the state flow diagram listed in the DS28E38 IC data sheet. There are nine device function commands that are summarized in Table 2 and are described in detail in subsequent sections. Within this flow diagram, the data transfer is verified when writing and reading by a CRC of 16-bit type (CRC-16). The CRC-16 is computed as described in Maxim Application Note 27.

Table 2. Device Function Command Summary

COMMAND	CODE	DESCRIPTION	TYPE
Command Start	66h	Start of the command sequence	Global
Write Memory	96h	Write memory page	General
Read Memory	44h	Read memory page	General
Read Status	AAh	Read the protection for each page and MANID	General
Set Page Protection	C3h	Set page protection	General
Compute and Read Page Authentication	A5h	Compute ECDSA authentication on page	ECDSA
Decrement Counter	C9h	Decrement counter	General
Device Disable	33h	Permanently disable device	General
Read RNG	D2h	Read RNG value	General
Generate ECC-256 Key Pair	CBh	Generate key pair and optional write protect	ECDSA

Command Start (66h)

The Command Start command has a flexible structure that is a jumping off point for device function commands that are powered by the 1-Wire. After the Command Start byte, the next byte transmitted is the length byte. This indicates the length of both the command (i.e., device function command) and parameters. The result of the command is returned in similar format. The Command Start structure does not require a strong pullup (SPU) until after the release byte. After the release byte, the command commences and a command-dependent delay is put into effect.

Table 3. Command Start Command

COMMAND CODE	66h
Parameter Byte(s)	Length byte followed by command and parameters. The first byte after the length byte is the device function command.
Usage	Process the command and parameters. The command code is followed by a length byte followed by the command and parameters. Following the write, a two-byte inverted CRC-16 of the command start byte + length byte + command + parameters is sent. If the CRC-16 is correct, the master then sends the release byte (AAh). Once the release byte is received, the command is started. At that time, the master must provide strong pullup on the 1-Wire to power the device. The required delay is command dependent with a minimum delay of 15ms. After the delay, the master must read a 1-byte "dummy" for clocking purposes. After the dummy byte, the command result is read, length byte first, followed by a result byte, optionally result data, and an inverted CRC-16. If the command is not supported, the response has a length of 00h followed by the CRC-16 FFFFh.
Command Restrictions	None
Device Operation	Verify release byte is 0xAA. Start command.
Command Duration	See t_{RM}, t_{WM}, t_{WS}, t_{GKP}, t_{GES}, and t_{ODC} (command dependent).
Result	Command dependent followed by inverted CRC-16. If the device is disabled, all commands result in an error result byte of 88h with length 1.

Table 4. Generic Command Start Sequence

Reset
Presence Pulse
<ROM Select>
Tx: Command Start (66h)
Tx: Length byte (varies with command)
Tx: Command
Tx: Parameters (varies with command)
Rx: CRC-16 (inverted of command start, length, command, and parameters)
Tx: Release Byte (AAh)
<SPU Delay, command dependent>
Rx: Dummy Byte (not used in CRC calculation)
Rx: Length byte (varies with command)
Rx: Result byte (varies with command)
Rx: Result data (varies with command)
Rx: CRC-16 (inverted of length byte, result byte, and result data)
Reset

Write Memory (96h)

The Write Memory command is used to write a 32-byte page. The page can be any EEPROM page (0–6). The page must not have WP or DC protection. If the page is protected, it fails with a 55h result byte. On success, the result byte is AAh. The 32-byte page data is provided after the parameter byte during the command sequence. The command provides an inverted CRC-16 verification before issuing the release byte to initiate the operation. All writes must be 32 bytes.

Table 5. Write Memory Command

COMMAND CODE	96h
Parameter Byte(s)	See below
Usage	A write is done by page number and always has a write size of 32 bytes. This function can also set the state of the decrement counter page 3 before DC protection is set. If the page protection is EM, then only allow 1 bit to be changed to 0.
Command Restrictions	Only valid on pages 0–6 without WP or DC protection.
Device Operation	Verify that the destination page does not have protection set (WP or DC). Write the data. Set the result byte.
Command Duration	t_{WM}
Result Byte	55h = The command failed because destination page is protected (WP). 77h = Invalid input or parameter 88h = Device disabled AAh = Success

Write Memory Parameter Byte

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
0	0	0	0	0	PAGE#		

Bits 2:0: Memory Page Number (PAGE#). Page to write, 0 to maximum page number of 6.

Table 6. Write Memory Sequence

Reset
Presence Pulse
<ROM Select>
Tx: Command Start (66h)
Tx: Length byte 34d
Tx: Command 96h (Write Memory)
Tx: Parameter
Tx: New page data (32d bytes)
Rx: CRC-16 (inverted of command start, length, command, parameter, new page data)
Tx: Release Byte
<Delay t_{WM}>
Rx: Dummy Byte
Rx: Length Byte (1d)
Rx: Result Byte
Rx: CRC-16 (inverted of length and result byte)
Reset

Read Memory (44h)

The Read Memory command is used to read a 32-byte page. EEPROM page (0–5) can be read if RP protection is not set for the page. EEPROM page 6 has intrinsic RP protection. If the page is read protected, it fails with a 55h result byte followed by 32 FFh bytes. All reads are the full 32 bytes. On success, the result byte is AAh.

Table 7 Read Memory Command

COMMAND CODE	44h
Parameter Byte(s)	Page number to read
Usage	Read a page of memory. This function can also read the special purpose page 3 when decrement counter (DC) is set.
Command Restrictions	This command is applicable only to memory pages that do not have read protection.
Device Operation	Verify that the destination page does not have protection set (RP). Read the data
Command Duration	t_{RM}
Repeat Byte Error	55h = Page is read protected (RP) 77h = Invalid input or parameter 88h = Device disabled (result length 1) AAh = Success

Read Memory Parameter Byte

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
0	0	0	0	0	PAGE#		

Bits 2:0: Memory Page Number (PAGE#). These bits select the page number to be read. Acceptable values are from pages 0–6.

Table 8. Read Memory Sequence

Reset
Presence Pulse
<ROM Select>
Tx: Command Start (66h)
Tx: Length byte 2d
Tx: Command 44h (Read Memory)
Tx: Parameter (page)
Rx: CRC-16 (inverted of command start, length, command, and parameter)
Tx: Release Byte
<Delay t_{RM}>
Rx: Dummy Byte
Rx: Length (33d)
Rx: Result Byte
Rx: Read page data (32d bytes)
Rx: CRC-16 (inverted, length byte, result byte, and page data)
Reset

Read Status (AAh)

The Read Status command reads the protection state of all six memory pages, 2-byte MANID, and 2-byte device version, and can run the entropy health test. The command reports both intrinsic protection (RP private key) and values that have been set using Set Page Protection. This command can optionally do an entropy heath test and report the status. The health test is selected with a parameter byte and requires an additional delay to do the test.

Table 9. Read Status Command

COMMAND CODE	AAh
Parameter Byte(s)	See below (select optional entropy health test).
Usage	Read the page protection information for pages 0 to 6, MANID and two constant bytes 00h 01h representing the device version. Optionally, run an entropy heath test (i.e., on demand check) and report the result. The return result is always 13 bytes except for a disabled device (1 byte).
Command Restrictions	None
Device Operation	Read the page protection setting for all pages, read MANID, and perform entropy health test.
Command Duration	t_{RM} (status only) t_{RM} + t_{ODC} (status and entropy health test)
Repeat Byte Error	77h = Invalid parameter combination 88h = Device disabled (result length 1) AAh = Success

Read Status Parameter Byte

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
0	0	0	0	0	0	0	EHT

Bit 0: Entropy Health Test (EHT). Set to 1 to run the health test on the RNG. Set to 0 to not run the health test.

Page Protection Result Bitmap (for Each Page 0–6)

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
0	0	0	PF	DC	EM	WP	RP

Bit 4: PUF (PF). If PUF status bit is 1, the ECC-256 private PUF key is used directly. If the PUF status bit is 0, the PUF encrypted private key stored on page 6 is used.

Bit 3: Decrement Counter (DC). If DC is 1, this indicates the decrement counter is enabled and all other protection bits would not be applicable for page 3. If DC is 0, then the other protection settings apply as normal.

Bit 2: EPROM Emulation Mode (EM). This bit specifies whether the memory page is setup for EPROM Emulation mode, where writing is limited to changing bits from 1 to 0. If EM is 0 (factory default), the page can be written normally, provided that the page is not write-protected. If EM is 1, the EPROM Emulation mode is activated, provided that the memory page is not write-protected.

Bit 1: Write Protection (WP). This bit specifies whether the memory page is write-protected. If WP is 0 (factory default), the memory page is not protected. If WP is 1, the memory block is write-protected.

Bit 0: Read Protection (RP). This bit specifies whether the memory page is read-protected. If RP is 0 (factory default except for Page 6), the memory page is openly read-accessible through the Read Memory command. If RP is 1, the memory page's data is only internally accessible. Any read attempt reports FFh for each byte.

MANID (Byte 0)

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
MANID (LSByte)							

Bits 7:0: Manufacturing Identification (MANID). Provides the value of the MANID least-significant byte . See MANID (byte 1) for more details.

MANID (Byte 1)

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
MANID (MSByte)							

Bits 7:0: Manufacturing Identification (MANID). Provides the value of the MANID most-significant byte . The MANID is used to distinguish between devices that are factory preprogrammed (e.g., to install certain memory data) and user programmed. With user programmed parts, the MANID is 0000h. The MANID can be a customer-supplied identification code that assists the application software in identifying the product DS28E38 is associated with and in faster selection of public keys needed for verification. Contact the factory to set up and register a MANID.

DEVICE_VERSION (Byte 0)

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
DEVICE_VERSION (LSByte)							

Bits 7:0: Device Version (DEVICE_VERSION). This is the least-significant byte value of the device version.

DEVICE_VERSION (Byte 1)

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
DEVICE_VERSION (MSByte)							

Bits 7:0: Device Version (DEVICE_VERSION). This is the most-significant byte value of the device version.

Entropy Health Test Status

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
EHTS							

Bits 7:0: Entropy Health Test Status (EHTS). This the result of the EHTS byte being run on the RNG with the following three possible values:

FFh: test not performed

AAh: entropy healthy

DDh: entropy not healthy

Table 10. Read Status Sequence

Reset
Presence Pulse
<ROM Select>
Tx: Command Start (66h)
Tx: Length byte 2d
Tx: Command AAh (Read Status)
Tx: Parameter byte (entropy heath test select)
Rx: CRC-16 (inverted of command start, length, command, and parameter)
Tx: Release Byte
<Delay t_{RM} or t_{RM} + t_{ODC}>
Rx: Dummy Byte
Rx: Length Byte (13d)
Rx: Result Byte
Rx: Read protection values (7 bytes), MANID (2 bytes), DEVICE_VERSION (2 bytes), EHTS (1 byte)
Rx: CRC-16 (inverted, length byte, protection values, MANID, DEVICE_VERSION, EHTS byte)
Reset

Set Page Protection (C3h)

The Set Page Protection command sets the protection state of a single memory page or the two-page public key (pages 4 + 5). This is a one-time operation for each protection area with one exception. Page 6 with intrinsic RP+PF protection can be set to RP to specify the page 6 private key and changed back to the intrinsic RP+PF. However this is not possible if "WP" is already set. Other than this exception, attempting to set the protection of a page a second time results in an error 55h result byte. Attempting to set a protection combination on a protection area that is not valid results in a 77h error code. AAh is the result byte for a successful operation. When setting page 3 to decrement counter protection (DC), the upper 16 bytes of data are preserved, making it write-protected. Consequently, this area can be used for constant data written prior to setting the decrement counter.

Table 11. Set Page Protection Command

COMMAND CODE	C3h
Parameter Byte(s)	Two parameters. Byte 1, page to set protection. Byte 2, protection options.
Usage	Set protection. This is a one-time write of the page protection for each protection area. There are six protection areas: page 0, page 1, page 2, page 3, page 4+5, page 6. All protection modes for the area needed must be set in one function call.
Command Restrictions	Pages 0,1,2,4+5: RP, WP, EM, RP+WP, RP+EM Page 3: RP, WP, EM, RP+WP, RP+EM, DC Page 6: RP+WP, RP+PF, RP+PF+WP (RP+PF is set by default)
Device Restrictions	Verify that the destination Page does not already have protection set Verify that the protection requested is valid for the page area. Write the protection
Command Duration	t_{WS} (pages except page 3) $t_{WS} + t_{WM}$ (DC page 3 only)
Result Byte	77h = Invalid parameter combination 55h = The command failed because protection for the page was already done 88h = Device disabled (result length 1) AAh = Success

Set Page Protection Parameter (Byte 1)

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
0	0	0	0	0	PAGE#		

Bits 2:0: Memory Page Number (PAGE#). These bits select the page number to be protected. Acceptable values are from pages 0–6.

Set Page Protection Parameter (Byte 2)

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
0	0	0	PF	DC	EM	WP	RP

Bit 4: PUF (PF). This bit only applies to page 6. It specifies the private key source for the compute and read page authentication command. If PF is 0, page 6 data is used as the private key. If PF is 1, the PUF key is used as the private key. The private key can be permanently set to PUF and locked by setting PF+RP+WP for page 6. If WP is not set for page 6, PF can be set and reset, allowing the user to switch the private key between the page 6 data, and the PUF key. The default state of the PF bit is 1.

Bit 3: Decrement Counter (DC). This bit specifies whether memory page 3 is to be set up as a decrement counter. If DC is 0 (factory default), the memory page 3 is not a decrement counter but a user page. If DC is 1, the memory page becomes a 17-bit decrement counter that decrements by the decrement counter command with the upper 16 bytes of the page write protected.

Bit 2: EPROM Emulation Mode (EM). This bit specifies whether the memory page is to be setup for EPROM Emulation mode, where writing is limited to changing bits from 1 to 0. If EM is 0 (factory default), the page can be written normally, provided that the page is not write-protected. If EM is 1, the EPROM Emulation mode is activated. EPROM emulation mode is applicable to user pages, decrement counter page 3, and public key pages 4 and 5. This bit has no function with the private key page 6.

Bit 1: Write Protection (WP). This bit specifies whether the memory page is to be write-protected. If WP is 0 (factory default), the memory page is not protected. If WP is 1, the memory page becomes write-protected. This is applicable to user pages, decrement counter page 3, public key pages 4 and 5 and private key page 6.

Bit 0: Read Protection (RP). This bit specifies whether the memory page is to be read-protected. If RP is 0 (factory default is 1), the memory page is openly read-accessible through the Read Memory command. If RP is 1, the memory page's data becomes only internally accessible. This is applicable to user pages, decrement counter page 3, public key pages 4 and 5. Private key page 6 is an exception and this bit must always be set to 1 otherwise other protection bits can't be set.

Table 12. Set Page Protection Sequence

Reset
Presence Pulse
<ROM Select>
Tx: Command Start (66h)
Tx: Length byte
Tx: Command C3h (Set Page Protection)
Tx: Parameter (page)
Tx: Parameter (protection)
Rx: CRC-16 (inverted of command start, length, command, parameters)
Tx: Release Byte
<Delay t_{WS} or $t_{WS} + t_{WM}$>
Rx: Dummy Byte
Rx: Length Byte (1d)
Rx: Result Byte
Rx: CRC-16 (inverted, length byte and result byte)
Reset

Compute and Read Page Authentication (A5h)

The Compute and Read Page Authentication command creates an authentication response based on a provided challenge. This operation works without regard to any protection mode on the designated page (0–5). The authentication result is an ECDSA signature. Figure 2 shows the Compute and Read Page Authentication command block diagram. The 32-byte challenge is provided after the parameter byte in the command flow. Failure to compute a signature results in an error result byte 22h. The parameter includes the page number to use for the authentication and a flag to indicate anonymous mode. Anonymous mode sets the ROM ID in the computation to FFhs. An invalid parameter results in an error result byte 77h. The authentication result is read following the dummy byte and includes a length and result byte. The authentication message input format is shown in Table 15.

Table 13. Compute and Read Page Authentication Command

COMMAND CODE	A5h
Parameter Byte(s)	See below
Usage	Compute and read an authentication sequence on pages 0–5. In other words, this operation is to compute ECDSA signature on a page. The destination page does not need to have any protection mode. The 32-byte challenge is provided during the command flow following the parameter. The private key used to compute the ECDSA is either stored in page 6 or is the PUF if page 6 protection includes PF. The return value is a result byte followed by the 64-byte signature ('s' followed by 'r').
Command Restrictions	Private Key page 6 is not permitted.
Device Operation	Verify that the destination page is valid. Read 32-byte challenge from the command flow. Compute ECDSA signature based on challenge, ROMID, MANID, and Private Key (page 6 or PUF). Read the authentication result value (ECDSA signature). Set result byte.
Command Duration	t_{GES} (ECDSA signature duration)
Result Byte	22h = failure to create signature 77h = Invalid input or parameter 88h = Device disabled (result length 1) AAh = Success

Compute and Read Page Authentication Parameter Byte

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
ANON			0	0	PAGE#		

Bits 7:5: Anonymous Indicator (ANON). These bits specify whether the device's ROM ID is used for the ECDSA authentication computation. To use the ROM ID, these bits must be 000b. To make the ECDSA computation anonymous by replacing the ROM ID with FFh bytes, these bits must be 111b. All other codes are invalid and, if chosen, cause the parameter byte to be invalid.

Bits 2:0: Memory Page Number (PAGE#). These bits select the page number to be used as the data page for the ECDSA computation. An acceptable value is any page number from 0–5.

Table 14. Compute and Read Page Authentication Sequence

Reset
Presence Pulse
<ROM Select>
Tx: Command Start (66h)
Tx: Length byte 34d
Tx: Command A5h (Compute and Read Page Authentication)
Tx: Parameter (anonymous flag, page)
Tx: Challenge (32d bytes)
Rx: CRC-16 (inverted of command start, length, command, parameter, and challenge)
Tx: Release Byte
<Delay t_{GES}>
Rx: Dummy Byte
Rx: Length byte (65d)
Rx: Result Byte
Rx: Read ECDSA Signature (64 bytes, 's' and then 'r', MSByte first), signature 00hs if result byte is not AA success
Rx: CRC-16 (inverted, length byte, result byte, and signature)
Reset

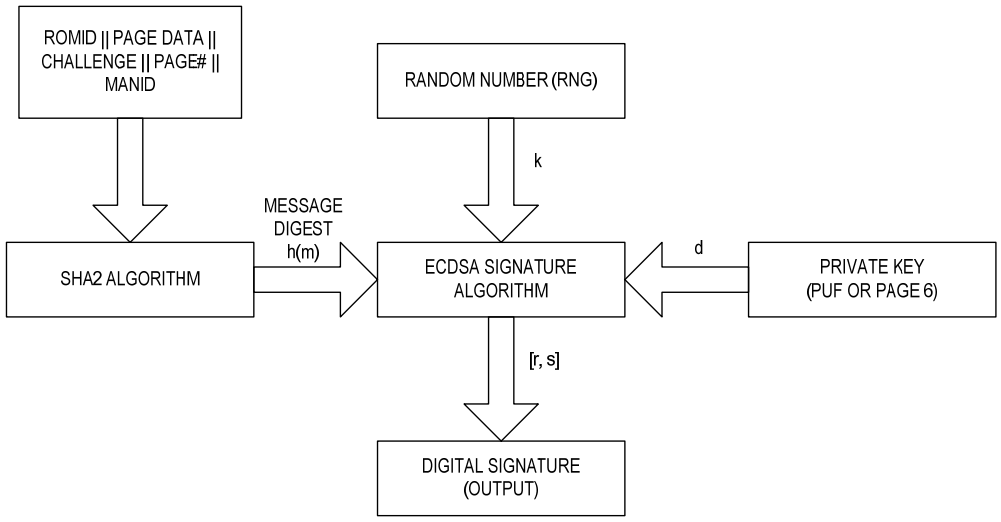

Figure 2. Compute and Read Page Authentication command block diagram.

Table 15. Compute and Read Page Authentication–ECDSA Hash Input–(ROM ID || Page Data || Challenge || Page# || MANID)

BYTE 0	BYTE 1	BYTE 2	BYTE 3	BYTE 4	BYTE 5	BYTE 6	BYTE 7
RN + 0	RN + 1	RN + 2	RN + 3	RN + 4	RN + 5	RN + 6	RN + 7
BYTE 8	BYTE 9	BYTE 10	BYTE 11	BYTE 12	BYTE 13	BYTE 14	BYTE 15
PD + 0	PD + 1	PD + 2	PD + 3	PD + 4	PD + 5	PD + 6	PD + 7
BYTE 16	BYTE 17	BYTE 18	BYTE 19	BYTE 20	BYTE 21	BYTE 22	BYTE 23
PD + 8	PD + 9	PD + 10	PD + 11	PD + 12	PD + 13	PD + 14	PD + 15
BYTE 24	BYTE 25	BYTE 26	BYTE 27	BYTE 28	BYTE 29	BYTE 30	BYTE 31
PD + 16	PD + 17	PD + 18	PD + 19	PD + 20	PD + 21	PD + 22	PD + 23
BYTE 32	BYTE 33	BYTE 34	BYTE 35	BYTE 36	BYTE 37	BYTE 38	BYTE 39
PD + 24	PD + 25	PD + 26	PD + 27	PD + 28	PD + 29	PD + 30	PD + 31
BYTE 40	BYTE 41	BYTE 42	BYTE 43	BYTE 44	BYTE 45	BYTE 46	BYTE 47
CH + 0	CH + 1	CH + 2	CH + 3	CH + 4	CH + 5	CH + 6	CH + 7
BYTE 48	BYTE 49	BYTE 50	BYTE 51	BYTE 52	BYTE 53	BYTE 54	BYTE 55
CH + 8	CH + 9	CH + 10	CH + 11	CH + 12	CH + 13	CH + 14	CH + 15
BYTE 56	BYTE 57	BYTE 58	BYTE 59	BYTE 60	BYTE 61	BYTE 62	BYTE 63
CH + 16	CH + 17	CH + 18	CH + 19	CH + 20	CH + 21	CH + 22	CH + 23
BYTE 64	BYTE 65	BYTE 66	BYTE 67	BYTE 68	BYTE 69	BYTE 70	BYTE 71
CH + 24	CH + 25	CH + 26	CH + 27	CH + 28	CH + 29	CH + 30	CH + 31
BYTE 72	BYTE 73	BYTE 74					
PG	MANID + 0	MANID + 1					

(RN + N) – Byte N of the 64-bit ROM ID; RN + 0 corresponds to the family code.
(PD + N) – Byte N of Page Data; $0 \leq N \leq 31$.
(CH + N) – Byte N of Challenge; $0 \leq N \leq 31$.
PG – Page number as in the parameter byte for this command; same as PAGE# field.
(MANID + N) – Byte N of the 16-bit manufacturer ID; MANID + 0 is the LSbyte.

Decrement Counter (C9h)

The Decrement Counter command takes the value in the 17-bit register on the decrement counter page 3, subtracts one and writes the value back. The Decrement Counter command value is set using the Write Memory command before applying the DC protection to page 3. If the DC protection is not set on page 3, the Decrement Counter command fails with an error 33h result byte. If the counter is at 0 and cannot be decremented, the error result bytes is 55h. 22h is returned for a general failure to decrement. AAh is the result byte for a successful operation.

Table 16. Decrement Counter Command

COMMAND CODE	C9h
Parameter Byte(s)	None
Usage	The Decrement Counter command is used to decrement the write-once 17-bit counter on the decrement counter on page 3. The counter must have already been written and the DC protection set on page 3. The operation fails if the counter is already zero. Note that if the counter protection is not yet set, then it fails with a 33h. A general failure to decrement the counter fails with return byte of 22h.
Command Restrictions	Decrement counter must have been set with Write Memory.
Device Operation	Verify counter has been set and is > 0. Decrement counter.
Command Duration	t_{WM}
Result Byte	55h = The command failed because the counter is already 0. 33h = Invalid sequence, required step not done (decrement counter page 3 does not have DC protection) 22h = Failure to decrement 88h = Device disabled AAh = Success

Table 17. Decrement Counter Sequence

Reset
Presence Pulse
<ROM Select>
Tx: Command Start (66h)
Tx: Length byte 1d
Tx: Command C9h (Decrement Counter)
Rx: CRC-16 (inverted of command start, length, command)
Tx: Release Byte
<Delay t_{WM}>
Rx: Dummy Byte
Rx: Length Byte (1d)
Rx: Result Byte
Rx: CRC-16 (inverted, length byte and result byte)
Reset

Table 18. Decrement Counter Page 3 Format

BYTE 0	BYTE 1	BYTE 2	BYTE 3	BYTE 4	BYTE 5	BYTE 6	BYTE 7
DCNT + 0	DCNT + 1	DCNT + 2	0	0	0	0	0
BYTE 8	BYTE 9	BYTE 10	BYTE 11	BYTE 12	BYTE 13	BYTE 14	BYTE 15
0	0	0	0	0	0	0	0
BYTE 16	BYTE 17	BYTE 18	BYTE 19	BYTE 20	BYTE 21	BYTE 22	BYTE 23
PD + 16	PD + 17	PD + 18	PD + 19	PD + 20	PD + 21	PD + 22	PD + 23
BYTE 24	BYTE 25	BYTE 26	BYTE 27	BYTE 28	BYTE 29	BYTE 30	BYTE 31
PD + 24	PD + 25	PD + 26	PD + 27	PD + 28	PD + 29	PD + 30	PD +31

(DCNT + N) - Byte N of decrement counter.

(PD + N) - Byte N of Page data (written prior to setting DC protection).

Device Disable (33h)

Command to permanently disable the device.

Table 19. Device Disable Command

COMMAND CODE	33h
Parameter Byte(s)	Release sequence is 8 bytes long.
Usage	Permanently disables the device. The command only proceeds if the release sequence is correct. The release sequence is an 8-byte value. The generic device has one value and the preprogramming devices have a custom value. Once a device is disabled, all device function commands result in an error result byte of 88h.
Command Restrictions	Preprogramming customers can request that this command be deactivated. Contact factory for more details.
Device Operation	Verify that the release sequence is correct. Disable the device.
Command Duration	t_{WS}
Result Byte	55h = Release sequence is incorrect 88h = Device disabled AAh = Success

Device Disable Parameter Bytes

BYTE 0	BYTE 1	BYTE 2	BYTE 3	BYTE 4	BYTE 5	BYTE 6	BYTE 7
9Eh	A7h	49h	FBh	10h	62h	0Ah	26h

Table 20. Device Disable Sequence

Reset
Presence Pulse
<ROM Select>
Tx: Command Start (66h)
Tx: Length byte 9d
Tx: Command 33h (Device Disable command)
Tx: Release Sequence (8 bytes)
Rx: CRC-16 (inverted of command start, length, command, and release sequence)
Tx: Release Byte
<Delay t_{WS}>
Rx: Dummy Byte
Rx: Length Byte (1d)
Rx: Result Byte
Rx: CRC-16 (inverted, length byte and result byte)
Reset

Read RNG (D2h)

Command to set the number of random bytes to be generated and read.

Table 21. Read RNG Command

COMMAND CODE	D2h
Parameter Byte(s)	Number of RNG bytes to read.
Usage	Compute and read random data from true RNG.
Command Restrictions	—
Command Duration	t_{CMP}
Result Byte	AAh = Success 77h = Invalid parameter

Read RNG Parameter Byte

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
0	0	NBR#					

Bits 5:0: Number of Random Bytes (NBR#). Number of random bytes to read minus 1.

Table 22. Read RNG Sequence

Reset
Presence Pulse
<ROM Select>
Tx: Command Start (66h)
Tx: Length Byte (2d)
Tx: Read RNG (D2h)
Tx: Parameter
Rx: CRC-16 (inverted of command start, length, command, and parameter)
Tx: Release Byte
< Delay t_{CMP}>
Rx: Dummy Byte
Rx: Length Byte (variable)
Rx: Result Byte
Rx: RNG data (variable bytes)
Rx: CRC-16 (inverted of length byte, result byte, and RNG data)
Reset

Generate ECC-256 Key Pair (CBh)

The Generate ECC-256 Key Pair command generates a key pair. The key pair can optionally be write protected upon completion of this operation. AAh is the result byte for a successful operation. The private key portion of the key pair can either be the PUF or a random value generated and stored in page 6. The private key option is selected with the parameter. If a user-specified key pair is desired, the Write Memory command is used to write the public key (pages 4 and 5) and the private key (page 6). To lock a user-specified key, use the Set Page Protection command.

Table 23. Generate ECC-256 Key Pair Command

COMMAND CODE	CBh
Parameter Byte(s)	Select lock enable and private key source.
Usage	The Generate ECC-256 Key Pair command is used to complete the ECC key set for authentication by using the PUF as the public key.
Command Restrictions	Can only be run once if lock enable selected. If page 6 (private key) already has PF protection enabled, the PUF selection must be used in the parameter (PRK = 1). If (PRK = 1), page 6 protection is set to PF and optionally WP (LE = 01b or 10b).
Device Operation	Verify public key and private key is not write protected. Read PUF (if PUF private key selected). Perform ECC public key generation using private key. Write the public key, optionally write the private key (PRK = 0). Optionally set write protection on both public key pages 4-5 and private key 6 (LE = 01b or 10b).
Command Duration	t_{GKP} (no lock) $t_{GKP} + t_{WS}$ (lock)
Result Byte	55h = The command failed because the key is write protected (locked). 22h = Invalid ECDSA input or result 88h = Device disabled AAh = Success

Generate ECC-256 Key Pair Parameter Byte

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
LE		0	0	0	0	0	PRK

Bits 7:6: Locking Enable (LE). These bits specify whether the key pair is to be automatically write protected (locked) after it is copied to key memory (page 4, 5, and 6). To leave the key pair open for later changes, these bits must be 00b or 11b. To make the key pair permanent (protect from changes), these bits must be 01b or 10b.

Bit 0: Private Key (PRK). This bit selects the private key to use being either a random number generated and saved in EEPROM page 6 or the PUF key. If the bit is 1, the PUF is the private key used when generating the ECC-256 key pair. If this bit is 0, a random number is generated and saved in the EEPROM, and is the private key used when generating the ECC-256 key pair.

Table 24. Generate ECC-256 Key Pair Sequence

Reset
Presence Pulse
<ROM Select>
Tx: Command Start (66h)
Tx: Length byte 2d
Tx: Command CBh (Generate ECC-256 Key Pair)
Tx: Parameter
Rx: CRC-16 (inverted of command start, length, command, parameter)
Tx: Release Byte
<Delay t_{GKP} or $t_{GKP} + t_{WS}$>
Rx: Dummy Byte
Rx: Length Byte (1d)
Rx: Result Byte
Rx: CRC-16 (inverted, length byte and result byte)
Reset

Trademarks

1-Wire is a registered trademark of Maxim Integrated Products, Inc.

ChipDNA is a trademark of Maxim Integrated Products, Inc.

Revision History

REV NUMBER	REV DATE	DESCRIPTION	PAGES CHANGED
0	9/17	Initial release	—