DS28E39 Security User Guide

UG6796; Rev 0; 10/18

Abstract

This security user guide contains detailed information about the device function commands of the DS28E39. It must be used in conjunction with its corresponding data sheet, which contains pin descriptions, feature overviews, and electrical specifications.

Table of Contents

List of Figures

List of Tables

General Information

The DS28E39 is an ECDSA public-key-based bidirectional secure authenticator that incorporates Maxim®'s patented ChipDNA™ technology, 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). This user guide must be used in conjunction with the corresponding DS28E39 data sheet.

After a 1-Wire® Reset/Presence cycle and ROM function command sequence is successful, the DS28E39 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 DS28E39. 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 DS28E39 sent after the dummy byte.

Usage Example

The following usage example provides a brief explanation of the commands required for typical application scenarios. The commands are broken up between a setup section and a usage section for each example. There are three sets of key pairs available for authentication and writing to the memory. The following is a brief description of each of the public keys and certificates.

Table 1. Public Key Pair and Certificate Definition

KEY NAME	DESCRIPTION
Device Certificate	Created certificate of the Device Public Key signed by the Authority Private Key.
Authority Public Key	Authority Public Key is generated by the system from the Authority Private Key and is saved to the DS28E39. This public key is used to verify all certificates to make sure the host or device is part of the secure system.
Write Public Key	Write Public Key is generated by the host from the Write Private Key that is stored and hidden in the host. This key is used to carry out the authenticated writes to the device in conjunction with the calculated Write Certificate.
Write Certificate	Created certificate with the Write Public Key signed by the Authority Private Key. This needs to be supplied to a device to write with authentication.
Device Public Key	Device Public Key is read by using the Read Device Public Key command. This public key is generated from the PUF private key when needed.

Setup

- Externally generate an ECC-256 Authority Key Pair for the system. This key pair is used to generate and verify all certificates to make sure the device or host is part of the secure system.
- Externally generate an ECC-256 Write Key Pair for the host. This write key pair is used to write with authentication to the device.
- Create the Write Certificate with the Write Public Keys signed by the Authority Private Key.
- On power-up, populate the ROM ID serial number with a Skip ROM command followed by a Read Status command.

- Perform Read Memory on ROM options page to get the ROM ID and MANID for a device certificate.
- Perform Read Device Public Key command to read the device public key for a device certificate.
- Perform Write Memory to write a device certificate, which is signed by the Verify Private Key, to the user pages to authenticate the device public key.
- Perform Set Page Protection to set WP on device certificate pages.
- Perform Write Memory on Authority Public Key.
- Perform Write Memory to set WP on Authority Public Key pages.
- Perform Write Memory to set data to user page(s).
- Perform Set Page Protection to set ECW on desired user page(s).

Read User Pages with Authentication Usage

- On power-up, retrieve the MANID and populate the ROM ID serial number with a Skip ROM command followed by a Read Status command.
- Read the ROM ID with a Read ROM command.
- Perform Read Device Public Key command for Device Public Key value.
- Perform Read Memory on user pages with a device certificate. The master verifies the device certificate of the Device Public Key.
- Perform Read Memory on user page(s).
- Perform Compute and Read Page Authentication on user page(s).
- Host verifies the signature with the Device Public Key.

Write to User Pages with Authentication Usage

- On power-up, retrieve the MANID and populate the ROM ID serial number with a Skip ROM command followed by a Read Status command.
- Read the ROM ID with a Read ROM command.
- Host writes the Write Public Key to the device with the Write Memory command.
- Perform Authenticate Public Key with Write Certificate and Authority Public Key that matches a page with ECW protection (this sets the W_PUB_KEY flag to allow authenticate writes with the Write Public Key). This certificate is created with the Authority Private Key.
- Perform Read Memory on user page (old data).
- Perform Authenticated Write Memory on desired user page (new data). The write authentication signature is created with the Write Private Key.

Memory Resources

The memory array of the DS28E39 is configured with nine pages of memory as shown in Table 2. Two of these pages are volatile and the other seven reside in the EEPROM array. The secured 2Kb EEPROM array has seven pages. The volatile memory of page 7 and page 8 are used for a temporary location to authorize a written public key. The first five of nine pages can be used for user memory or certificates with the protection setting support. Optionally, page 4 can be used for the decrement counter. Page 5 and page 6 are used for the authority public key X/Y and only have the option of write protect. Setting protection on either page 5 or page 6 automatically sets the other. The per-device unique ECDSA private/public key pair for signatures is derived from the ChipDNA output. The corresponding public key is read through a device command and computed by the DS28E39 when requested by a host controller. A certificate for the public key is computed externally during an initialization step and stored in user memory pages. Each page of memory is 32 bytes.

Table 2. Memory Map with Optional Protections (32-Byte Pages)

PAGE	REGION	MEMORY TYPE	DEFAULT PROTECTION	OPTIONAL PROTECTION
0–3	User Memory/Certificates	EE	—	RP, WP, EM, ECW
4	User Memory/Certificates/ Decrement Counter	EE	—	RP, WP, EM, ECW, DC
5, 6	Authority Public Key X/Y	EE	—	WP
7, 8	Write Public Key	Volatile	—	N/A

Table 3. Protection Types

PROTECTIONS TYPES	
PROTECTION	DESCRIPTION
RP	Read protect
WP	Write protect
ECW	Authentication write protection ECDSA
EM	EPROM emulation (only set bits to 0)
DC	17-bit decrement counter enabled on page 4

64-Bit ROM ID

Each DS28E39 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.

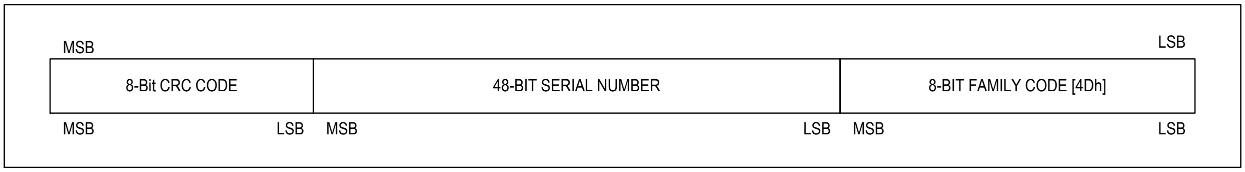


Figure 1. 64-bit ROM ID.

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 DS28E39 IC data sheet. The Command Start command and the eleven device function commands are summarized in Table 4 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 4. 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
Read Device Public Key	CBh	Generates the device Public Key from the Private Key	ECDSA
Authenticate Public Key	59h	Verifies that the loaded Write Public Key is authentic	ECDSA
Authenticate Write	89h	Writes with authentication using ECDSA	ECDSA

Command Start (66h)

The Command Start command has a flexible structure that initiates device function commands. 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 5. Command Start Command Descriptions

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 6. 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 page (0–8). The page must not have WP, ECW, 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 7. Write Memory Command Descriptions

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 4 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 0–8 without WP, ECW, or DC protection.
Device Operation	Verify that the destination page does not have protection set (WP, ECW, 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	PAGE#			

Bits 3:0: Memory Page Number (PAGE#). Page to write, 0 to maximum page number of 8.

Table 8. 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. Page 0–8 can be read if RP protection is not set for the page. 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 9. Read Memory Command Descriptions

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 4 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	PAGE#			

Bits 3:0: Memory Page Number (PAGE#). These bits select the page number to be read. Acceptable values are from pages 0–8.

Table 10. 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 seven EEPROM memory pages, 2-byte MANID, and 2-byte device version and can run the entropy health test. The command reports the 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. The command also reports the device version. This can be used to differentiate this device from the DS28E38 since both devices use the same family code.

Table 11. Read Status Command Descriptions

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 07h 00h 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	ECW	DC	EM	WP	RP

Bit 4: Authentication Write Protection ECDSA (ECW). If ECW bit is 1, the memory page requires ECDSA authentication for writes. If ECW bit is 0, the memory page is not protected by this bit.

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 4. 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, 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 DS28E39 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. The DS28E39 device is 07h.

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. The DS28E39 device is 00h.

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 12. 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 authority public key (page 5 and page 6). This is a one-time operation for each protection area. 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 4 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 13. Set Page Protection Command Descriptions

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, and page 5+6. All protection modes for the area needed must be set in one function call.
Command Restrictions	Pages 0-3: RP, WP, EM, RP+WP, RP+EM, ECW, ECW+RP, ECW+EM, ECW+RP+EM Page 4: RP, WP, EM, RP+WP, RP+EM, DC, ECW, ECW+RP, ECW+EM, ECW+RP+EM Page 5+6: WP (Setting WP to one page sets the same protection to the other.)
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 4) t_{WS} + t_{WM} (DC on page 4 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	ECW	DC	EM	WP	RP

Bit 4: Authentication Write Protection ECDSA (ECW). If ECW is 1, the memory page requires ECDSA authentication for writes. If ECW is 0, the memory page is not protected by this bit.

Bit 3: Decrement Counter (DC). This bit specifies whether memory page 4 is to be set up as a decrement counter. If DC is 0 (factory default), the memory page 4 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 and decrement counter page 4.

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 4, and public key page 5 and 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), 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 and decrement counter page 4.

Table 14. 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 (0–6). 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 17.

Table 15. Compute and Read Page Authentication Command Descriptions

COMMAND CODE	A5h
Parameter Byte(s)	See below
Usage	Compute and read an authentication sequence on pages 0-6. This operation computes an ECDSA signature on a specified 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 the PUF private key. The return value is a result byte followed by the 64-byte signature ('s' followed by 'r').
Command Restrictions	The volatile memory pages of 7 and 8 are 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 PUF Private Key. Read the authentication result value (ECDSA signature). Set result byte.
Command Duration	t_{GES} (ECDSA signature duration)
Result Byte	22h = failure to create signature (Once set requires POR to clear in subsequent command calls) 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 0–6.

Table 16. 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

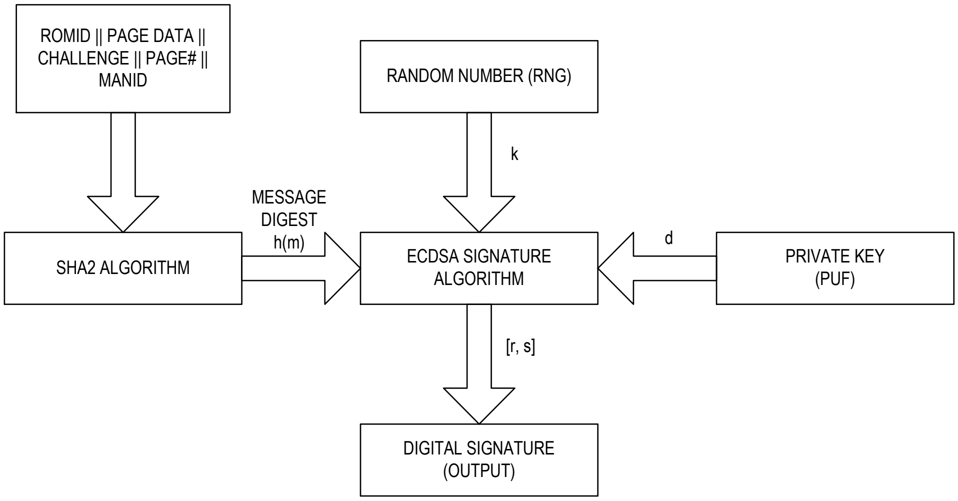

ROMID || PAGE DATA || CHALLENGE || PAGE# || MANID
RANDOM NUMBER (RNG)
k
MESSAGE DIGEST h(m)
SHA2 ALGORITHM
ECDSA SIGNATURE ALGORITHM
d
PRIVATE KEY (PUF)
[r, s]
DIGITAL SIGNATURE (OUTPUT)

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

Table 17. Compute and Read Page Authentication – Compute SHA-256 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 ≤ N ≤ 31.

(CH + N) – Byte N of Challenge; 0 ≤ N ≤ 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 4, 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 4. If the DC protection is not set on page 4, 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 18. Decrement Counter Command Descriptions

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 4. The counter must have already been written and the DC protection set on page 4. 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 4 does not have DC protection) 22h = Failure to decrement 88h = Device disabled AAh = Success

Table 19. 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 20. Decrement Counter Page 4 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 21. Device Disable Command Descriptions

COMMAND CODE	**33h**
Parameter Byte(s)	Release sequence is 8 bytes long.
Usage	Permanently disables the device. The command only proceeds if the Device Disable Parameter Byte sequence is correct. The parameter byte 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 22. Device Disable Sequence

Reset
Presence Pulse
<ROM Select>
Tx: Command Start (66h)
Tx: Length byte 9d
Tx: Command 33h (Device Disable command)
Tx: Device Disable Parameter Bytes (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 23. Read RNG Command Descriptions

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	77h = Invalid parameter AAh = Success

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 24. 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

Read Device Public Key (CBh)

The Read Device Public Key command reads the device public key generated by the PUF private key.

Table 25. Read Device Public Key Command Descriptions

COMMAND CODE	**CBh**
Parameter Byte(s)	None
Usage	The Read Device Public Key command is used to read back the Device Public Key for authentication. The PUF Private key is used each time to generate the Device Public Key.
Command Restrictions	None
Device Operation	Generate the corresponding public key from the PUF-based private key.
Command Duration	t_{GkP}
Result Byte	22h = Invalid ECDSA input or result (Once set requires POR to clear in subsequent command calls) 88h = Device disabled AAh = Success

Table 26. Read Device Public Key Sequence

Reset
Presence Pulse
<ROM Select>
Tx: Command Start (66h)
Tx: Length byte 1d
Tx: Command CBh (Read Public Key)
Tx: Parameter
Rx: CRC-16 (inverted of command start, length, command, parameter)
Tx: Release Byte
<Delay t_{GKP}>
Rx: Dummy Byte
Rx: Length Byte (65d)
Rx: Result Byte
Rx: Public Key X (32d)
Rx: Public Key Y (32d)
Rx: CRC-16 (inverted, length byte and result byte)
Reset

Authenticate Public Key (59h)

The Authenticate Public Key command is used to verify that the provided signature (certificate) matches the public key that is preloaded in Write Public Key location with the Authority Public Key.

Table 27. Authenticate Public Key Command Descriptions

COMMAND CODE	**59h**
Parameter Byte(s)	Certificate, Certificate Customization
Usage	The Write Public Key is used to authenticate writes. If the certificate (i.e. Write Certificate) is verified, the status bit 'W_PUB_KEY' is set indicating that Write Public Key is authorized to authenticate ECDSA writes to the pages protected with ECW. The public key used to verify the signature is the Authority Public Key.
Command Restrictions	Certificate Customization Parameter length is valid from 1 to 32 bytes.
Device Operation	The flag 'W_PUB_KEY' is set indicating that the Write Public Key is authorized to authenticate ECDSA writes to the pages protected with ECW. 'W_PUB_KEY' flag is cleared on any write to Write Public Key or cleared if the result byte is not AAh when this command is executed.
Command Duration	t_{VES}
Result Byte	22h = Compute failure during signature verification (Once set requires POR to clear in subsequent command calls) 77h = Invalid input or parameter 00h = Failure to verify signature (Once set requires POR to clear in subsequent command calls) AAh = Success

Table 28. Authenticate Public Key Sequence

Reset
Presence Pulse
<ROM Select>
Tx: Command Start (66h)
Tx: Length Byte (variable, depends on length of customization)
Tx: Authenticate Public Key Command (59h)
Tx: Certificate Parameter (64d bytes) [r and then s, MSByte first]
Tx: Certificate Customization Parameter (variable from 1 to 32 bytes)
Rx: CRC-16 (inverted of command start, length, command, and parameters)
Tx: Release Byte
<Delay t_{VES}>
Rx: Dummy Byte
Rx: Length Byte (1d)
Rx: Result Byte
Rx: CRC-16 (inverted of length byte and result byte)
Reset

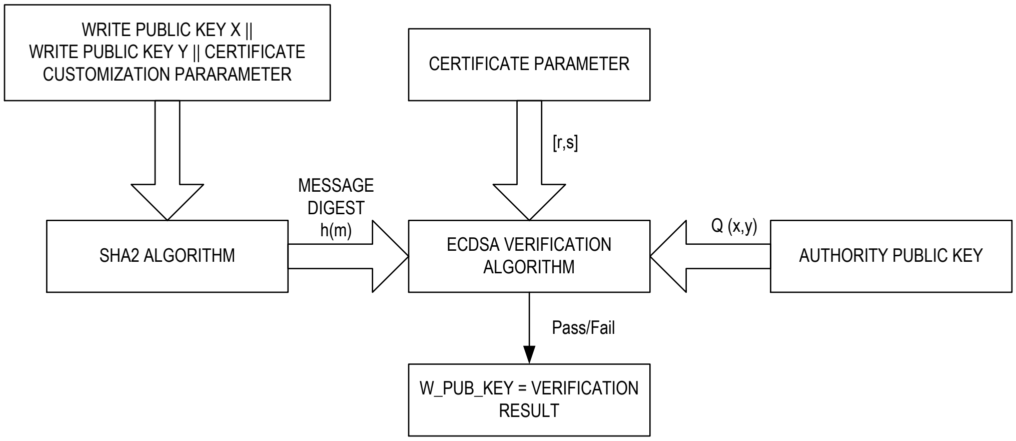


Figure 3. Authenticate Public Key (operation to authorize Write Public Key for writes)

Table 29. Authenticate Public Key – Compute SHA-256 Hash Input (Write Public Key X || Write Public Key Y || Certificate Customization)

BYTE 0	BYTE 1	BYTE 2	BYTE 3	BYTE 4	BYTE 5	BYTE 6	BYTE 7
PSX + 0	PSX + 1	PSX + 2	PSX + 3	PSX + 4	PSX + 5	PSX + 6	PSX + 7
BYTE 8	BYTE 9	BYTE 10	BYTE 11	BYTE 12	BYTE 13	BYTE 14	BYTE 15
PSX + 8	PSX + 9	PSX + 10	PSX + 11	PSX + 12	PSX + 13	PSX + 14	PSX + 15
BYTE 16	BYTE 17	BYTE 18	BYTE 19	BYTE 20	BYTE 21	BYTE 22	BYTE 23
PSX + 16	PSX + 17	PSX + 18	PSX + 19	PSX + 20	PSX + 21	PSX + 22	PSX + 23
BYTE 24	BYTE 25	BYTE 26	BYTE 27	BYTE 28	BYTE 29	BYTE 30	BYTE 31
PSX + 24	PSX + 25	PSX + 26	PSX + 27	PSX + 28	PSX + 29	PSX + 30	PSX + 31
BYTE 32	BYTE 33	BYTE 34	BYTE 35	BYTE 36	BYTE 37	BYTE 38	BYTE 39
PSY + 0	PSY + 1	PSY + 2	PSY + 3	PSY + 4	PSY + 5	PSY + 6	PSY + 7
BYTE 40	BYTE 41	BYTE 42	BYTE 43	BYTE 44	BYTE 45	BYTE 46	BYTE 47
PSY + 8	PSY + 9	PSY + 10	PSY + 11	PSY + 12	PSY + 13	PSY + 14	PSY + 15
BYTE 48	BYTE 49	BYTE 50	BYTE 51	BYTE 52	BYTE 53	BYTE 54	BYTE 55
PSY + 16	PSY + 17	PSY + 18	PSY + 19	PSY + 20	PSY + 21	PSY + 22	PSY + 23
BYTE 56	BYTE 57	BYTE 58	BYTE 59	BYTE 60	BYTE 61	BYTE 62	BYTE 63
PSY + 24	PSY + 25	PSY + 26	PSY + 27	PSY + 28	PSY + 29	PSY + 30	PSY + 31
BYTE 64	BYTE 65					BYTE 64 + CS_LEN - 1	BYTE 65 + CS_LEN
CS + 0	CS + 1					CS + CS_LEN - 1	CS + CS_LEN

(PSX + N) – Byte N of Write Public Key; 0 ≤ N ≤ 31.

(PSY + N) – Byte N of Write Public Key; 0 ≤ N ≤ 31.

(CS + N) – Byte N of Certificate Customization.

CS_LEN – Length of Certificate Customization; 1 <= CS_LEN <= 32.

Authenticated Write Memory (89h)

Writes with authentication using ECDSA.

Table 30. Authenticated Write Memory Command Descriptions

COMMAND CODE	89h
Parameter Byte(s)	Page, New Page Data, Authentication Signature.
Usage	Writes new page data to a memory page with ECW protection. Prior to using this function, a successful call to Authenticate Public Key command must be done to set W_PUB_KEY. Then an Authentication Signature can be used with this command to write the new data.
Command Restrictions	This command is applicable only to memory pages that already have ECDSA write protection (ECW). Requires W_PUB_KEY to be set.
Device Operation	The Authenticated Write Memory writes new page data if the Authentication Signature (Signed by the Write Private Key in the application) verifies with the Write Public Key while the W_PUB_KEY is set.
Command Duration	$t_{VES} + t_{WM}$
Result Byte	22h = ECDSA verification failed (Once set requires POR to clear in subsequent command calls) 33h = The command failed because master authentication is required (W_PUB_KEY not set) 55h = Invalid sequence, required step not done. 77h = Invalid input or parameter 00h = Invalid ECDSA signature authorization parameter (Once set requires POR to clear in subsequent command calls) AAh = Success

Authenticated 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#). 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 0–4.

Table 31. Authenticated Write Memory Sequence

Reset
Presence Pulse
<ROM Select>
Tx: Command Start (66h)
Tx: Length byte 98d
Tx: Authenticated Write Memory (89h)
Tx: Page Parameter
Tx: New Page Data Parameter (32d bytes)
Tx Authentication Signature Parameter (64d byte) [r and then s, MSByte first]
Rx: CRC-16 (inverted of command start, length, command, and parameters)
Tx: Release Byte
<Delay $t_{VES} + t_{RM}$ >
Rx: Dummy Byte
Rx: Length byte (1d)
Rx: Result Byte
Rx: CRC-16 (inverted, length byte, result byte)
Reset

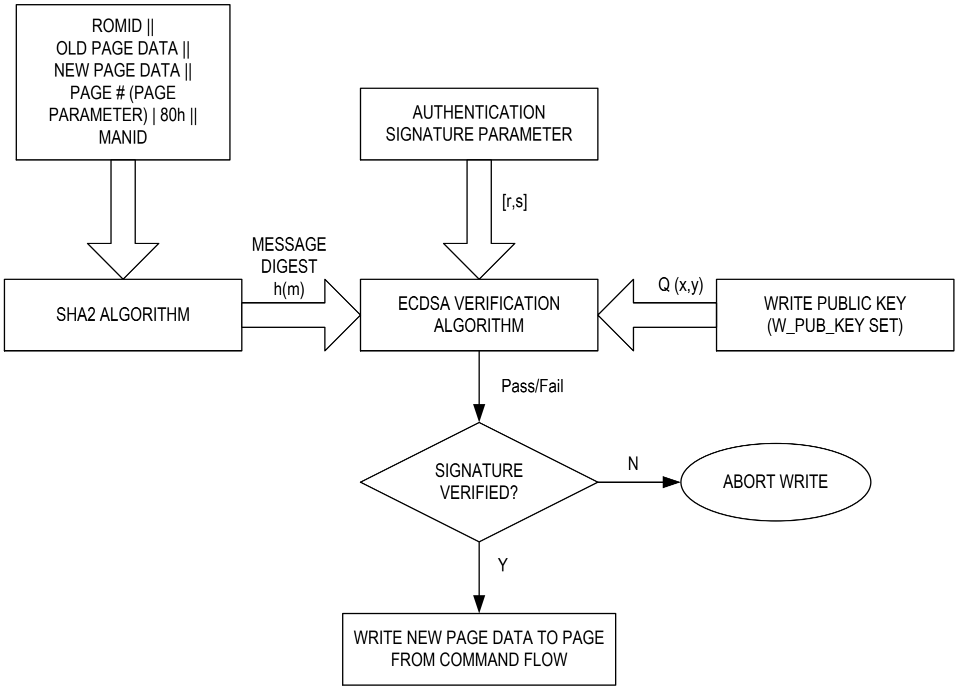


Figure 4. Authenticated Write Memory (operation to authenticate signature for ECDSA Write).

Table 32. Authenticated Write Memory–Compute SHA-256 Hash Input (ROM ID || Old Page Data || New Page Data || 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
OP + 0	OP + 1	OP + 2	OP + 3	OP + 4	OP + 5	OP + 6	OP + 7
BYTE 16	BYTE 17	BYTE 18	BYTE 19	BYTE 20	BYTE 21	BYTE 22	BYTE 23
OP + 8	OP + 9	OP + 10	OP + 11	OP + 12	OP + 13	OP + 14	OP + 15
BYTE 24	BYTE 25	BYTE 26	BYTE 27	BYTE 28	BYTE 29	BYTE 30	BYTE 31
OP + 16	OP + 17	OP + 18	OP + 19	OP + 20	OP + 21	OP + 22	OP + 23
BYTE 32	BYTE 33	BYTE 34	BYTE 35	BYTE 36	BYTE 37	BYTE 38	BYTE 39
OP + 24	OP + 25	OP + 26	OP + 27	OP + 28	OP + 29	OP + 30	OP + 31
BYTE 40	BYTE 41	BYTE 42	BYTE 43	BYTE 44	BYTE 45	BYTE 46	BYTE 47
NP + 0	NP + 1	NP + 2	NP + 3	NP + 4	NP + 5	NP + 6	NP + 7
BYTE 48	BYTE 49	BYTE 50	BYTE 51	BYTE 52	BYTE 53	BYTE 54	BYTE 55
NP + 8	NP + 9	NP + 10	NP + 11	NP + 12	NP + 13	NP + 14	NP + 15
BYTE 56	BYTE 57	BYTE 58	BYTE 59	BYTE 60	BYTE 61	BYTE 62	BYTE 63
NP + 16	NP + 17	NP + 18	NP + 19	NP + 20	NP + 21	NP + 22	NP + 23
BYTE 64	BYTE 65	BYTE 66	BYTE 67	BYTE 68	BYTE 69	BYTE 70	BYTE 71
NP + 24	NP + 25	NP + 26	NP + 27	NP + 28	NP + 29	NP + 30	NP + 31
BYTE 72	BYTE 73	BYTE 74					
80h | PG	MANID + 0	MANID + 1					

(RN + N) – Byte N of the 64-bit ROM ID; RN + 0 corresponds to the family code.

(OP + N) – Byte N of Old Page; 0 ≤ N ≤ 31.

(NP + N) – Byte N of New Page; 0 ≤ N ≤ 31.

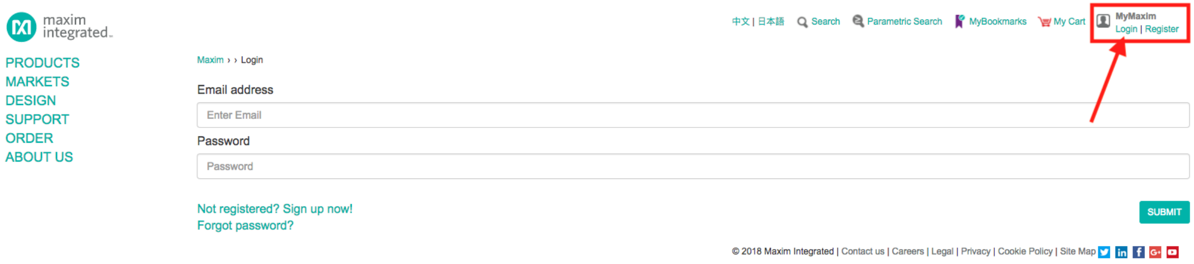
PG – Page number

(MANID + N) – Byte N of the 16-bit manufacturer ID; MANID + 0 is the LSbyte.

Appendix: DS28E39 Evaluation Kit Developer Software

Perform the following steps to download the DS28E39 EV kit developer software.

1. Log in to your My Maxim account.



Email address

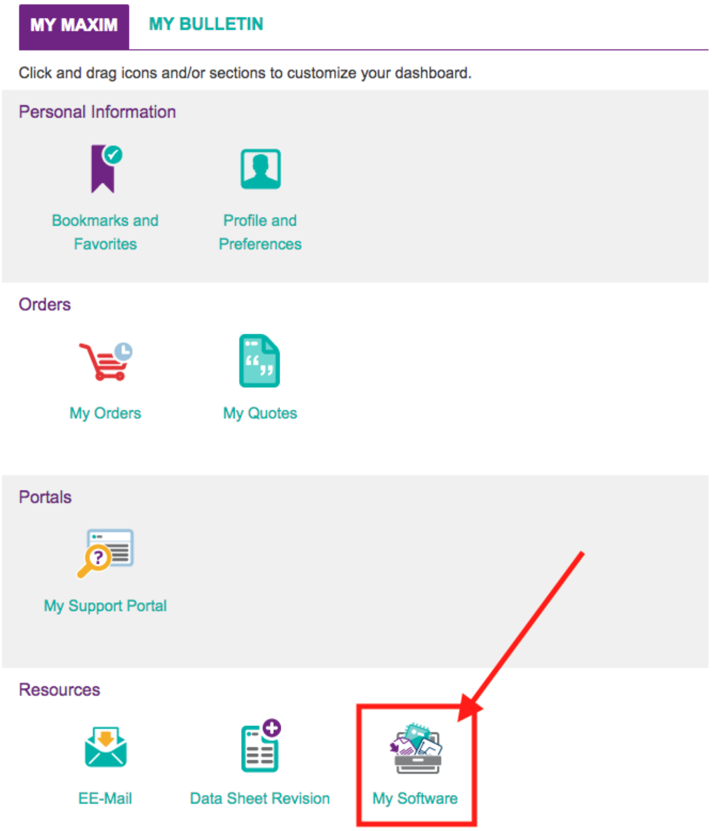
Enter Email

Password

Password

Figure 5. My Maxim account login.

2. After logging in, click on the "My Maxim" hyperlink underneath your name in the upper right corner of the page.
3. In the window that pops up, click on the "My Software" button as shown in the screenshot below.



Click and drag icons and/or sections to customize your dashboard.

Figure 6. My software.

4. Select DS28E39 EV Kit Developer Software from the list of available software and wait for the download to complete in your browser.

Trademarks

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

ChipDNA is a trademark of Maxim Integrated Products, Inc.

Maxim is a registered trademark of Maxim Integrated Products, Inc.

MAXIM INTEGRATED CONFIDENTIAL

Revision History

REV NUMBER	REV DATE	DESCRIPTION	PAGES CHANGED
0	10/18	Initial release	—