#### Evaluates: DS28C40

#### **General Description**

The DS28C40 evaluation system (EV system) provides the hardware and software necessary to exercise the features of the DS28C40. The EV system consists of five DS28C40 devices in a 10-pin TDFN package, a DS9121CQ+ evaluation TDFN socket board, and a DS9481P-300# USB-to-I<sup>2</sup>C/1-Wire<sup>®</sup> adapter. The evaluation software runs under Windows<sup>®</sup> 10, Windows 8, and Windows 7 operating systems, both 64- and 32-bit versions. It provides a handy user interface to exercise the features of the DS28C40.

#### **Features**

- Demonstrates the Features of the DS28C40 DeepCover Secure Authenticator
- Logs 1-Wire/I<sup>2</sup>C Communication to Aid Firmware Designers Understanding of DS28C40
- 1-Wire/I<sup>2</sup>C USB Adapter Creates a Virtual COM Port on Any PC

#### DS28C40 EV System with a USB Cable

- Fully Compliant with USB Specification v2.0
- Software Runs on Windows 10, Windows 8, and Windows 7 for Both 64- and 32-Bit Versions
- 3.3V ±3% I<sup>2</sup>C Operating Voltage
- Convenient On-Board Test Points, TDFN Socket
- Evaluation Software Available by Request

#### **EV Kit Contents**

QTY	DESCRIPTION
5	DS28C40Q+ DeepCover secure authenticator with (10 TDFN)
1	DS9121CQ+ socket board (10 TDFN)
1	DS9481P-300# USB to 1W/I <sup>2</sup> C Adapter
1	USB Type-A to USB Mini Type-B cable

#### Ordering Information appears at end of data sheet.



DeepCover is a registered trademark of Maxim Integrated Products, Inc. Windows is registered trademarks of Microsoft Corp. Windows is a registered trademark and registered service mark of Microsoft Corporation.



#### Evaluates: DS28C40

#### **Quick Start**

This section is intended to give the DS28C40 evaluator a list of recommended equipment and instructions on how to set up the Windows-based computer for the evaluation software.

#### **Recommended Equipment**

- DS9481P-300# USB to 1W/I<sup>2</sup>C Adapter
- DS9121CQ+ TDFN socket board
- DS28C40Q+ (five devices included)
- USB Type A-to-USB Micro-Type B cable (included)
- Computer with a Windows 10, Windows 8, or Windows 7 operating system (64- or 32-bit) and a spare USB 2.0 or higher port
- DS28C40 EV kit software. If needed go to the Maxim website and search for the DS28C40 EV kit.

Click the **Design Resources** link. Then click the **DS28C40EVKIT Software Lite** link to download the **DS28C40\_Evaluation\_Kit\_Lite\_Version\_Setup\_** V1\_2\_0.zip file or newer version software.

**Note:** In the following sections, EV kit software related items are identified in **bold**. Windows operating system related items are identified in **bold and underline**.

# Hardware Setup and Driver Installation Quick Start

The following steps were performed on a Windows 7 PC to setup the DS28C40 EV kit hardware/software:

- 1) Obtain and unpack DS28C40\_Evaluation\_Kit\_Lite\_ Version\_Setup\_V1\_2\_0.zip file or newer version.
- In a file viewer, double click on the DS28C40\_ Evaluation\_Kit\_Lite\_Version\_Setup\_V1\_2\_0 to begin the installation.



Figure 1. File Viewer

- 3) The setup wizard opens. Click on <u>Next</u> (Figure 2):
- 4) Click <u>Next</u> (Figure 3) to install to the default folder.

maxim integrated.	Welcome to the DS28C40 Evaluation Kit Lite Version Setup Wizard
	This will install DS28C40 Evaluation Kit Lite Version version 1_2_0 on your computer.
	It is recommended that you close all other applications before continuing.
	Click Next to continue, or Cancel to exit Setup.

Figure 2. DS28C40 Setup Wizard

Select Destination Location Where should DS28C40 Evaluation	on Kit Lite Version be installed?	
Setup will install DS28C4	Ю Evaluation Kit Lite Version into the follow	ing folder.
To continue, dick Next. If you we	ould like to select a different folder, click Bro	owse.
m Files (x86)\Maxim Integrated	DS28C40 Evaluation Kit Lite Version B	rowse
At least 17.2 MB of free disk space	ce is required.	
	< Back Next >	Cancel

Figure 3. Install Folder Location

- 5) Click <u>Next</u> to install shortcuts to the default folder (Figure 4).
- 6) Unplug any Maxim adapter and click on <u>Next</u> (Figure 5) with the default settings checked. This action installs the DS9481P-300 driver that is needed to communicate through the USB by a virtual COM port.

🗴 Setup - DS28C40 Evaluation Kit Lite Version — 🗌 🗙
Select Start Menu Folder Where should Setup place the program's shortcuts?
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, dick Next. If you would like to select a different folder, dick Browse.           Maxim Integrated\DS28C40 Evaluation Kit Lite Version         Browse
Don't create a Start Menu folder
< Back Next > Cancel

Figure 4. Program Shortcuts Location

Which additional tasks should be performed?		
Select the additional tasks you would like Setup f Evaluation Kit Lite Version, then dick Next. Install DS948 1P-300 driver Additional icons: Create desktop icon Start menu icons: Create uninstall icon	perform while installing DS28	C40
☑ Create uninstall icon		

Figure 5. Select to Install the Driver

- 7) Next click on **Install** (Figure 6). A new window pops up to show progress of the installation.
- 8) Click on <u>Next</u> (Figure 7) when the Device Driver Installation Wizard appears.

your computer.	
Click Install to continue with the installation, or click Back if you want to review or change any settings. Destination location: C:\Program Files (x86)\Maxim Integrated\DS28C40 Evaluation Kit Lite Version Start Menu folder: Maxim Integrated\DS28C40 Evaluation Kit Lite Version Additional tasks: Install DS9481P-300 driver Start menu icons: Create uninstall icon	

Figure 6. Ready to Install

Welcome to the Device Driver Installation Wizard! This wizard helps you install the software drivers that some
To continue, click Next
To continue, click Next.

Figure 7. Device Driver

- 9) Click on <u>Finish</u> (Figure 8) to close the final window confirming the driver was installed correctly.
- 10) Now that the driver is installed, connect the hardware by doing the following:
  - a) Open the socket and insert a DS28C40 into one of the cavities, as shown in <u>Figure 9</u>. Note: The plus (+) on the package must be on aligned with the top of the marker in the socket.
- b) Close the clamshell socket.
- c) Connect the DS9121CQ J2, 10-pin male plug, into the DS9481P-300#, 10-pin female socket (Figure 10).
- d) For the DS9121CQ+, insert jumper JB1 to use VCC (Figure 10).
- e) Plug-in the DS9481P-300# using USB Type-A to USB Micro Type-B cable into the PC.



Figure 8. Device Driver Installed Finished



Figure 9. Orientation of the DS28C40 in the Clamshell Socket

#### Evaluates: DS28C40



11) Click on **Finish** (Figure 11) to close the final window confirming the software was installed correctly.

Figure 10. DS9481QA-300 and DS9121CQ

maxim integrated.	Completing the DS28C40 Evaluation Kit Lite Version Setup Wizard
	Setup has finished installing DS28C40 Evaluation Kit Lite Version on your computer. The application may be launched b selecting the installed icons.
	Click Finish to exit Setup.
	Launch DS28C40 Evaluation Kit Lite Version

Figure 11. Software Installation Finished

12) The DS28C40 EV kit program now opens and connects to the DS9481P-300 COM port. This can be verified in the lower right corner of the window as shown in Figure 12.

#### **Available Options**

The DS28C40 EV Kit Lite Program is designed as a usage example to show step by step how to use the

DS28C40 device. This version includes options to write, read, and run a compute authentication page using SHA2 or ECDSA. To access the full potential of the DS28C40, request the full version available under NDA request.

The GUI displays all the I<sup>2</sup>C sequences for each step performed to assist the firmware engineer.

#### DS28C40Deep Cover Secure Authentic File Tools Help Setup General Commands SHA2 Commands ECDSA Commands Select Command Select Page Adapter Part # DS9481P-300 Command OTP User Memory: Page 0 Status Connected on COM6 Page Data Search Adapter Set Protection 🗹 Secret A 🛛 📄 Secret B Read RNG Search Devices ECDSA Protection SHA2/Simple Protection Read RNG Parameter (NBR#) 1 RP-Read Protect DS28C40 WP-Write Protect EM-EPROM Emulation Mode Selected Device APH-Authentication Write Protection HMAC ROM ID EPH-Encryption and Authenticated Write Protection HMAC 1D000102030405E9 MAN ID 0000 Execute Command Log 🗹 Display I2C Log <SUCCESS> //Device found with ROMID: 1D000102030405E9 Deep Cover Secure Authenticator EV Kit Software (Lite Version)Rev: (1.2.0) Ready Connected on: COM6

Figure 12. DS28C40 EV Kit Program (Default View upon Opening)

#### Evaluates: DS28C40

#### **Usage Example—Feature Write Memory and Read Memory**

- 1) Select the **General Commands** tab (Figure 13).
- 2) Select the Write Memory command from the combo box selection (Figure 13).

up 🥑	General Commands SHA2 Commands ECDSA Commands	
Adapter Part # DS9/810-200	Select Command Select Page	
Status Connected on COME	Write Memory V OTP User Memory: Page 0 V	
Status Connected on COM6	Write Memory	
Search Adapter	AA 00 00 00 00 00 00 00 00 00 00 00 00 0	
	Set Protection Secret A Secret B Read RNG	
Search Devices	SHA2/Simple Protection     ECDSA Protection     Read RNG Parameter (NBR#)	
DS28C40	RP-Read Protect	
~	WP-Write Protect	
	C EM-EPROM Emulation Mode	
Selected Device	APH-Authentication Write Protection HMAC	
ROM ID	EPH-Encryption and Authenticated Write Protection HMAC	
1D000102030405E9		
MAN ID		
0000		
	Execute Command	
Display 12C Log		
[41] [21] [AA] [00] [00] [00] [00] [02] [19] [0	01] [72] [56] [19] [80] [D7] [00] [00] [00] [00] [00] [00] [00] [0	
SUCCESS>		

Figure 13. Selecting Command

## Evaluates: DS28C40

up <	General Commands SHA2 Commands ECDSA Commands	
Adapter Part # DS9481P-300 Status Connected on COM6	Select Command     Select Page       Write Memory     OTP User Memory: Page 0       Page Data	
Search Adapter	AA AA 00 00 00 00 00 00 00 00 00 00 00 0	
	Set Protection Secret A Secret B Read RNG	
S528C40 ✓	SHA2/Simple Protection     ECDSA Protection     Read RNG Parameter (NBR#)      RP-Read Protect     WP-Write Protect     EM-EPROM Emulation Mode	
ROM ID 10000102030405E9 MAN ID	EPH-Encryption and Authenticated Write Protection HMAC	
	Execute Command	
🗹 Display I2C Log		
[41] [21] [AA] [00] [00] [00] [00] [02] [19] [ SUCCESS> /Device found with ROMID: 1D0001020304	D1] [72] [56] [19] [80] [D7] [00] [00] [00] [00] [00] [00] [00] [0	

3) Write the desired data on the **Page Data** textbox (Figure 14).

Figure 14. Write Data

## Evaluates: DS28C40

4) Select the page for writing (Figure 15).

tup <	General Commands SHA2 Command	ds ECDSA Commands	
Adapter Part # DS9491D-200	Select Command	Select Page	
	Write Memory ~	OTP User Memory: Page 0	
Status Connected on COM6	Page Data	OTP User Memory: Page 0	
Search Adapter	AA AA 00 00 00 00 00 00 00 00 00 00 00 0	0 OTP User Memory: Page 2 OTP User Memory: Page 3	
	Set Protection	OTP User Memory: Page 4 OTP User Memory: Page 5	
DS28C40	SHA2/Simple Protection     RP-Read Protect     WP-Write Protect     WP-Write Protect	OTP User Memory: Page 6 OTP User Memory: Page 7 OTP User Memory: Page 8 OTP User Memory: Page 9	
Selected Device ROM ID 1D000102030405E9	APH-Authentication Write Prote	ection HMAC ted Write Protection HMAC	
MAN ID 0000		Execute Command	
✓ Display I2C Log			

Figure 15. Select Page

- 5) Click the **Execute Command** button (Figure 16). The I<sup>2</sup>C communication is displayed on the **Log** window and aids to understand how the command is executed.
- 6) To perform a memory read, in the **General Commands** tab, select the command from the **Select Command** dropdown menu (Figure 13).
- 7) From the Select Page drop-down menu, select the desired page to read (Figure 15).
- 8) Click the **Execute Command** button (Figure 16).

tup	General Commands SHA2 Commands ECDSA Commands	
Adveto-Destation Destation and	Select Command Select Page	
Adapter Part # DS9481P-300	Write Memory V OTP User Memory: Page 0 V	
Status Connected on COM6	Page Data	
Search Adapter	AA AA 00 00 00 00 00 00 00 00 00 00 00 0	
	Set Protection Secret A Secret B Read RNG	
Search Devices	SHA2/Simple Protection     ECDSA Protection     Read RNG Parameter (NBR#)	
DS28C40	RP-Read Protect	
~	WP-Write Protect	
Selected Device	APH-Authentication Write Protection HMAC	
100010202040559	EPH-Encryption and Authenticated Write Protection HMAC	
MANID		
0000		
	Execute Command	
M Display I2C Log		
S [41] [21] [AA] [00] [00] [00] [00] [02] [19] [0:	] [72] [56] [19] [80] [D7] [00] [00] [00] [00] [00] [00] [00] [0	
//Device found with ROMID: 1D00010203040.	5E9	

Figure 16. Execute Command

#### **Usage Example—SHA2 Compute and Read Page Authentication**

- 1) Under the General Commands tab, in the Select Command drop-down menu, select Write Memory (Figure 13).
- 2) Select the Secret A or B from Select Page drop-down menu for writing (Figure 17).
- 3) Write the desired secret on the Page Data text box and click Execute Command button (Figure 18).
- 4) Select the SHA2 Commands tab.
- 5) Select the **Compute and Read Page Authentication** command from the **Select Command** drop-down menu selection (Figure 19).

e Tools Help				
etup	General Commands SHA2 Commands	ECDSA Commands		
Adapter Part # DS9481P-300	Select Command	Select Page		
Status Connected on COM6	Write Memory ~	OTP User Memory: Page 0 🗸 🗸 🗸		
Status Connected on Comb	Page Data	OTP User Memory: Page 4 ^ OTP User Memory: Page 5		
Search Adapter	00 00 00 00 00 00 00 00 00 00 00 00 00	OTP User Memory: Page 6 OTP User Memory: Page 7		
	Set Protection	OTP User Memory: Page 8 OTP User Memory: Page 9		
Search Devices	SHA2/Simple Protection	OTP User Memory: Page 10 OTP User Memory: Page 11	(NBR#) 1	
DS28C40	RP-Read Protect	Page 38, Secret A		
~	WP-Write Protect	Page 39, Secret B		
	✓ EM-EPROM Emulation Mode			
Selected Device	APH-Authentication Write Protor	tion UMAC		
BOM ID				
10000102030405E9	EPH-Encryption and Authenticate	ed Write Protection HMAC		
MANID		I		
0000				
		Execut	te Command	
🗹 Display I2C Log				
\$ [41] [21] [AA] [00] [00] [00] [00] [FD] [07] [8 <success></success>	E2] [C7] [BD] [BE] [80] [3A] [00] [00] [00] [00	] [00] [00] [00] [00] [01] [00] [00] [00	04] [05] [E9] P	í literatura de la companya de la co
//Device found with ROMID: 1D00010203040	05E9			

Figure 17. Selecting SHA2 Command

Setup <	General Commands SHA2 Commands ECDSA Commands	
Adapter Part # DS9481P-300	Select Command Select Page	
Status Connected on COM6	Write Memory V Page 38, Secret A V	
status connected on como	Page Data	
Search Adapter	AA 00 00 00 00 00 00 00 00 00 00 00 00 0	
	Set Protection Secret A Secret B Read RNG	
Search Devices	SHA2/Simple Protection     BECDSA Protection     Read RNG Parameter (NBR#)	
DS28C40	RP-Read Protect	
~	WP-Write Protect	
	CEN-EPROM Emulation Mode	
Selected Davice	APL Authoritication Write Protection UMAC	
ROM ID	FPH Security and Authority and Authority Bestantian URAC	
1D000102030405E9	EPH-Endryption and Autoenticated write Protection Hidac	
MANID		
0000		
	Execute Command	
og 🕑 Display 12C Log		
.og ♥ Display 12C Log S [41] [21] [AA] [00] [00] [00] [00] [FD] [07] [E <success> //Device found with ROMID: 1D00010203040</success>	2] [C7] [BD] [BE] [80] [3A] [00] [00] [00] [00] [00] [00] [00] [0	,

Figure 18. Selecting SHA2 Command

		Commands	
Adapter Part # DS9481P-300	Select Command	Select Page	
Status Connected on COM6	Compute and Read Page Authentication	OTP User Memory: Page 0 ~	
Described on the second	Al: Authentication Type	Challenge	
Search Adapter		E1 9D E9 12 29 1B C5 B3 BC A1 A0 CF 59 BF	
	HMAC using SHA2 Secret A	FF 2E 87 BC 54 C7 0B 23 B0 FA 10 64 2C EF 56 36 DF 45	
Search Devices	HMAC using SHA2 Secret B	Generate Challenge	
DS28C40	HMAC Using SHA2 Secret S	Generate Ghaneinge	
~	Page Data	New Page Data	
	02 20 00 00 00 00 00 00 00 00 00 00 00 0	00 00 00 00 00 00 00 00 00 00 00 00 00	
Selected Device	00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00	
ROM ID			
1D000102030405E9	Secret A	Destination Secret (WPE) Lock Secret	
MAN ID		Secret A      Secret B      Secret S	
0000		00 00 00 00 00 00 00 00 00 00 00 00 00	
			Execute Command
Dicplay 130 Log			
S Dishiak 150 rog			
/ [28] [95] [3B] [42] [28] [2C] [F2] [6E]			
Command Result			

Figure 19. Selecting SHA2 Command

## Evaluates: DS28C40

6) From the **Select Page** drop-down menu, select a page to execute the command (Figure 20).

General Commands SHA2 Commands ECDSA	Commands	
Select Command	Select Page	
Compute and Read Page Authentication $\sim$	OTP User Memory: Page 0 🗸 🗸	
AT: Authentication Type	OTP User Memory: Page 0  OTP User Memory: Page 1	
HMAC using SHA2 Secret A     HMAC using SHA2 Secret B     HMAC Using SHA2 Secret S	OTP User Memory: Page 2           OTP User Memory: Page 3           OTP User Memory: Page 4           OTP User Memory: Page 5           OTP User Memory: Page 6           OTP User Memory: Page 7           OTP User Memory: Page 8	
Page Data	OTP User Memory: Page 9	
02 20 00 00 00 00 00 00 00 00 00 00 00 0	00 00 00 00 00 00 00 00 00 00 00 00 00	
Secret A	Destination Secret (WPE) Lock Secret	
	Secret A      Secret B      Secret S	
00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00	Command
	General Commands         SHA2 Commands         ECDSA           Select Command	General Commands       SHA2 Commands         Select Command       Select Page         Compute and Read Page Authentication Type       OTP User Memory: Page 0         OTP User Memory: Page 1       OTP User Memory: Page 1         OTP User Memory: Page 2       OTP User Memory: Page 3         OTP User Memory: Page 4       OTP User Memory: Page 5         OTP User Memory: Page 6       OTP User Memory: Page 6         OTP User Memory: Page 7       OTP User Memory: Page 7         OTP User Memory: Page 8       OTP User Memory: Page 9         Page Data       Other Memory: Page 9       O         Do co

Figure 20. Select Page

## Evaluates: DS28C40

-

7) In the AT: Authentication Type combo box, select a secret to compute the HMAC on selected page (Figure 21).

tup <	General Commands SHA2 Commands ECDSA	Commands	
Adapter Part # DS9481P-300	Select Command	Select Page	
Status Connected on COM6	Compute and Read Page Authentication 🗸 🗸	OTP User Memory: Page 0 ~	
	AT: Authentication Type	Challenge	
Search Adapter	HMAC using SHA2 Secret A     HMAC using SHA2 Secret B	E1 9D E9 12 29 1B C5 B3 BC A1 A0 CF 59 BF FF 2E 87 BC 54 C7 0B 23 B0 FA 10 64 2C EF 56 36 DF 45	
DS28C40	Page Data	New Page Data	
Selected Device		- 00 00 00 00 00 00 00 00 00 00 00 00 00	
1D000102030405E9	Secret A	Destination Secret (WPE) Lock Secret	
MAN ID 0000	00 00 00 00 00 00 00 00 00 00 00 00 00	Secret A     Secret B     Secret S	Execute Command
✓ Display I2C Log // [28] [95] [38] [42] [28] [2C] [F2] [6E] //Command Result			

Figure 21. Select Secret

## Evaluates: DS28C40

8) Click the Generate Challenge button to create a random challenge for command (Figure 22).

up	General Commands SHA2 Commands ECDSA	Commands	
Adapter Part # DS9481P-300	Select Command	Select Page	
Status Connected on COM6	Compute and Read Page Authentication $\sim$	OTP User Memory: Page 0 v	
	AT: Authentication Type	Challenge	
Search Adapter	HMAC using SHA2 Secret A	E1 9D E9 12 29 1B C5 B3 BC A1 A0 CF 59 BF FF 2E 87 BC 54 C7 0B 23 B0 FA 10 64 2C EF 56 36 DE 45	
Search Devices	HMAC Using SHA2 Secret S	Generate Challenge	
DS28C40	Page Data	New Page Data	
Selected Device	02 20 00 00 00 00 00 00 00 00 00 00 00 0	00 00 00 00 00 00 00 00 00 00 00 00 00	
1D000102030405E9	Secret A	Destination Secret (WPE) Lock Secret	
MAN ID		Secret A      Secret B      Secret S	
0000	00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00	Execute Command
✓ Display 12C Log / [28] [95] [38] [42] [28] [2C] [F2] [6E]			
//Command Result <success></success>			

Figure 22. Generate Challenge

#### Evaluates: DS28C40

9) Click the **Execute Command** button to run the sequence (Figure 23). The command result is displayed on the **Log** box.

up S	General Commands SHAZ Commands ECDSA	Commands	
Adapter Part # DS9481P-300	Select Command	Select Page	
Status Connected on COM6	Compute and Read Page Authentication $\sim$	OTP User Memory: Page 0 ~	
	AT: Authentication Type	Challenge	
Search Adapter	HMAC using SHA2 Secret A	E1 9D E9 12 29 1B C5 B3 BC A1 A0 CF 59 BF FF 2E 87 BC 54 C7 0B 23 B0 FA 10 64 2C EF	
Search Devices	<ul> <li>HMAC using SHA2 Secret B</li> <li>HMAC Using SHA2 Secret S</li> </ul>	Generate Challenge	
V	Page Data	New Page Data	
Selected Device	02 20 00 00 00 00 00 00 00 00 00 00 00 0	00 00 00 00 00 00 00 00 00 00 00 00 00	
1D000102030405E9	Secret A	Destination Secret (WPE) Lock Secret	
MANID		Secret A      Secret B      Secret S	
0000	00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00	Execute Command
Display 12C Log     [72] [95] [38] [42] [28] [2C] [F2] [6E]     [72] [72] [72] [72] [72] [72] [72] [			

Figure 23. Execute Command

#### Usage Example—ECDSA Compute and Read Page Authentication

- 1) Select the ECDSA Commands tab (Figure 24).
- 2) From the Select Command drop-down menu, select the Generate ECC-256 Key Pair and select the desired Public/ Private Key from the Key Selection combo box (Figure 24).

up	General Commands SHA	2 Commands ECDSA Commands			
Adapter Part # DS9481P-300 Status Connected on COM6 Search Adapter Search Devices DS28C40	Serect Command Generate ECC-256 Key Pail Compute and Read Page A Public Key AX 00 00 00 00 00 00 00 00 00 00 Public Key AY 00 00 00 00 00 00 00 00 00 Compute Multi-Block HAS Inout Data A Hey Forr	Page Page	> 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Key Selection  Public/Private Key A  Public/Private Key B  Hash Input Type	ECDH WR C 0 1 CS Offset 0 +
Selected Device ROM ID 1D000102030405E9 MAN ID 0000	ECDSA Signature r    s (he	ex)		32 Bytes Hash     32 Bytes Hash     SHA-256 from Data     Temporary Hash THASH from Set GPIO State on Valid Certificat     GPIO PIOA State Enable	n Multi-block :e New GPIO PIOA State Value 🔘 :
✓ Display I2C Log					Execute Command
:Delay 30ms> 5 (41] [21] [AA] [00] [00] [00] [00] [D5] [22] [	E2] [78] [C4] [C3] [79] [F5] [00]	[00] [00] [00] [00] [00] [00] [00] [01] [00] [00	1D] [00] [01] [02] [0	93] [04] [05] [E9] P	

Figure 24. Generate ECC Key pair

## Evaluates: DS28C40

	Select Command	Select Page		Key Colonian	
Adapter Part #     DS9481P-300       Status     Connected on COM6       Search Adapter	Generate ECC-256 Key I           Private Key A           00 00 00 00 00 00 00 00 00 00           Public Key AX           00 00 00 00 00 00 00 00 00 00 00			e Public/Private Key A	ECDH WR 0 0 1 CS Offset 0 +
Search Devices	Public Key AY 00 00 00 00 00 00 00 00 00	0 00 00 00 00 00 00 00 00 00 00 00 00 0	0 00 00 00 00 00 00 00 00 00		
Selected Device ROM ID 10000102030405E9 MAN ID 0000	Input Data • Hex F	ormat      String Format  (hex.)		32 Bytes Hash     32 Bytes Hash     SHA-256 from Data     Temporary Hash THASH fro Set GPIO State on Valid Certifica     GPIO PIOA State Enable	m Multi-block te New GPIO PIOA State Value 🍈
✓ Display I2C Log					Execute Command
5 [41] [21] [AA] [00] [00] [00] [00] [D5] [22] [	E2] [7B] [C4] [C3] [79] [F5] [0	0] [00] [00] [00] [00] [00] [00] [00] [	0] [00] [00] [1D] [00] [01] [02] [4	03] [04] [05] [E9] P	

3) Click the Execute Command button (Figure 25).

Figure 25. Execute Generate ECC Key

#### Evaluates: DS28C40

4) In the Select Command drop-down menu, select the Compute and Read Page Authentication command and the Public/Private Key from the Key Selection combo box (Figure 26).

E Key A a Key B CS Offset 0 ¢
e Key A a Key B CS Offset 0 ‡
e Key A e Key B 0 1 CS Offset 0 1 CS Offset
CS Offset
0 ÷
Data
Data
ash THASH from Multi-block
Valid Cartificata
vand Certificate
state Enable New GPIO PIOA State value 🕖
Even to Command
Execute command
Execute Comm
m 

Figure 26. Selecting Command

- 5) From the Select Page drop-down menu, select the desired page and public key (Figure 27).
- 6) From the AT: Authentication Type combo box, select the private key (Figure 27).
- 7) Click the **Generate Challenge** button and then click **Execute Command** button to perform the sequence (Figure 28). Results are displayed in the **Log** box.

Setup	General Commands SHA2 Commands ECDSA Com	mands	
Adapter Part # DS9481P-300 Status Connected on COM6 Search Adapter Search Devices DS28C40 Selected Device ROM ID ID000102030405E9 MAN ID 0000	Select Command Select Command Compute and Read Page Authentication Private Key A 000 00 00 00 00 00 00 00 00 00 00 00 00	82 Compute a	nd Read Page Authentication Options Current Page Data           00 00 00 00 00 00 00 00 00 00 00 00 00
Log 🕑 Display 12C Log	A) [51] [76] [16] [97] [D2] [00] [00] [00] [00] [00] [00] [00] [0	0) [01] [00] [00] [00] [1D] [00] [01] [02] [03] [04] [05] [	Execute Command

Figure 27. Selecting Page and Key

Adapter Part # DS9481P-300 Status Connected on COM6	Select Command Select Page	Compute and Read Page Authentication Options
Search Adapter Search Devices DS28C40 Selected Device ROM ID D000102030405E9 MAN ID 0000 D 000 MAN ID 0000 MAN ID	Lompute and Kead Page Authentication >         [0] P User Memory: Page 0         >           100 000 000 000 000 000 00 00 00 00 00 0	Current Page Data <u>for 20 00 00 00 00 00 00 00 00 00 00 00 00 </u>

Figure 28. Execute Command

#### Evaluates: DS28C40

#### Navigating

The DS28C40 EV Kit Lite Program is divided in five sections: the top menu bar, **Setup** panel, tab control, **Log**, and the status bar.

- **Menu Bar:** Provides additional software features and information used to support the software operation.
- **Setup Panel:** Information for hardware connection and device status.
- **Command Panel:** Main section for command execution and command option selection.
- Log: Software communication results for all commands and software transaction. Shows the I<sup>2</sup>C results and command's inputs and results.
- **Status Bar:** Displays the state of the software after connection the hardware necessary for operation

#### **Connecting and Detecting Hardware**

The DS28C40 EV Kit Lite Program detects automatically the required hardware on initialization. To exercise a different DS28C40, open the DS9121CQ socket and replace the device (Figure 9). Then click the **Search Device** button to detect then new DS28C40.

If, for any reason, the DS9481P-300 is not detected during the initial software load, click the **Search Adapter** button to detect and initialize the USB adapter.

## Evaluates: DS28C40

#### **Ordering Information**

PART	TYPE
DS28C40EVKIT#	EV System

#Denotes RoHS compliance.

#### **DS9121CQ EV Kit Bill of Materials**

DESIGNATION	QTY	DESCRIPTION			
Pack-Out	1	I2C AUTHENTICATOR AUTO, EV KIT DS28C40EVKIT#			
Pack-Out	5	AUTOMOTIVE I2C AUTHENTICATOR, 6Kb DS28C40G/V+			
Pack-Out	1	CABLE, USB A-TO-MICRO-B CABLE (1M) 68784-0001			
Pack-Out	1	1W/I2C 4x3MM TDFN SOCKET BOARD DS9121CQ+			
Pack-Out	1	BOX, BROWN, 9 3/16" X 7" X 1 1/4"			
Pack-Out	1	FOAM, ANTI-STATIC PE 12X12X3.175MM			
Pack-Out	2	LABEL, SATIN 1-3/4" X 1-3/8"			
Pack-Out	1	2X3", STATISHIELDING, ZIPTOP			
Pack-Out	1	INSERT+, MAXIM WEB INSTRUCTION			
Pack-Out	1	DS9481P-300 EVAL KIT# DS9481P-300#			
Pack-Out	1	1W/I2C 4X3MM TDFN SOCKET BOARD DS9121CQ+			
DS9121CQ+ PCB	1	1 PCB+, DS9121CQ+			
J4	1	CONN HEADER VERT 10POS 2.54MM 22284103			
J2	0.1	CONN+,HEADER,50PS, 100 SGL, R/A, AU TSW-150-08-G-S-RA			

DESIGNATION	QTY	DESCRIPTION			
J1	1	CONN+, RCPT, 100" 6POS, R/A GOLD PPPC061LGBN-RC			
U1	1	SOCKET+, IC, TDFN10, 4X3MM, CLAMSHELL 10QH50A14030-D			
PACK-OUT	1	LABEL BLANK THT-1-423 0.75 X 0.25			
PACK-OUT	1	BAG, STATIC SHIELDZIP4X6, W/ESD LO			
C1	1	CAP+, 0.1µF, 10%, 10V, X7R, 0603 C0603C104K8RACTU			
D1	1	LED+,GREEN CLEAR, 3.2V,20MA,0603 598-8081-107F			
JB1	0.1	HEADER 36-40 PINS (CUT TO FIT) 22-28-4363			
Populate to JB1	1	SHUNT+, LP W/HANDLE 2 POS 30AU 881545-2			
Q1	1	MOSFET, N-CH ENHANCEMENT BSS138LT1G			
R3	1	3.3KΩ 1% RESISTOR (0603 PB FREE) ERJ-3EKF3301V			
R1, R5	2	RES,10KΩ 1% 0603 ERJ-3EKF1002V			

#### **DS28C40 EV Kit Schematic**



#### DS28C40 EV Kit PCB Layout Diagrams



Drill and Mechanical Layer (1 of 3)

#### Evaluates: DS28C40



#### DS28C40 EV Kit PCB Layout Diagrams (continued)

Drill and Mechanical Layer (2 of 3)



Drill and Mechanical Layer (3 of 3)

#### Evaluates: DS28C40

#### **Revision History**

REVISION	REVISION	DESCRIPTION	PAGES
NUMBER	DATE		CHANGED
0	6/19	Initial release	

For pricing, delivery, and ordering information, please visit Maxim Integrated's online storefront at https://www.maximintegrated.com/en/storefront/storefront.html.

Maxim Integrated cannot assume responsibility for use of any circuitry other than circuitry entirely embodied in a Maxim Integrated product. No circuit patent licenses are implied. Maxim Integrated reserves the right to change the circuitry and specifications without notice at any time.



Компания «ЭлектроПласт» предлагает заключение долгосрочных отношений при поставках импортных электронных компонентов на взаимовыгодных условиях!

Наши преимущества:

- Оперативные поставки широкого спектра электронных компонентов отечественного и импортного производства напрямую от производителей и с крупнейших мировых складов;
- Поставка более 17-ти миллионов наименований электронных компонентов;
- Поставка сложных, дефицитных, либо снятых с производства позиций;
- Оперативные сроки поставки под заказ (от 5 рабочих дней);
- Экспресс доставка в любую точку России;
- Техническая поддержка проекта, помощь в подборе аналогов, поставка прототипов;
- Система менеджмента качества сертифицирована по Международному стандарту ISO 9001;
- Лицензия ФСБ на осуществление работ с использованием сведений, составляющих государственную тайну;
- Поставка специализированных компонентов (Xilinx, Altera, Analog Devices, Intersil, Interpoint, Microsemi, Aeroflex, Peregrine, Syfer, Eurofarad, Texas Instrument, Miteq, Cobham, E2V, MA-COM, Hittite, Mini-Circuits, General Dynamics и др.);

Помимо этого, одним из направлений компании «ЭлектроПласт» является направление «Источники питания». Мы предлагаем Вам помощь Конструкторского отдела:

- Подбор оптимального решения, техническое обоснование при выборе компонента;
- Подбор аналогов;
- Консультации по применению компонента;
- Поставка образцов и прототипов;
- Техническая поддержка проекта;
- Защита от снятия компонента с производства.



#### Как с нами связаться

**Телефон:** 8 (812) 309 58 32 (многоканальный) **Факс:** 8 (812) 320-02-42 **Электронная почта:** <u>org@eplast1.ru</u> **Адрес:** 198099, г. Санкт-Петербург, ул. Калинина, дом 2, корпус 4, литера А.