DS28C36/DS28E36 Evaluation System

Evaluates: DS28C36/DS28E36 and DS2476

General Description

The DS28C36/DS28E36 evaluation system (EV system) provides the hardware and software necessary to evaluate the DS28C36/DS28E36 and DS2476. The EV system consists of five DS28C36/DS28E36/DS2476 devices in a 6-pin TDFN package, a DS9121AQ+ evaluation TDFN socket board, and a DS9481P-300# USB-to-I2C/1-Wire® adapter. The evaluation software runs on Windows® 10, Windows 8, and Windows 7 operating systems (64- and 32-bit versions). The EV system provides a handy user interface to exercise the features of the DS28C36/DS28E36 and DS2476.

EV System Contents

QTY	DESCRIPTION
5	Includes five DS28C36Q+ or DS28E36Q+ DeepCover Secure Authenticators (6-pin TDFN)
5	DS2476Q+ DeepCover Secure Coprocessor (6-pin TDFN)
1	DS9121AQ+ socket board (6-pin TDFN)
1	DS9481P-300# USB-to-I2C/1-Wire Adapter
1	USB Type-A to USB Mini Type-B cable

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

Benefits and Features

- Demonstrates the Features of the DS28C36/DS28E36 DeepCover® Secure Authenticator
- Demonstrates the Features of the DS2476 DeepCover Secure Coprocessor
- I2C and 1-Wire Communication is Logged to Aid Firmware Designers Understanding of the DS2476, DS28C36, and DS28E36
- I2C/1W-USB Adapter Creates a Virtual COM Port on Any PC
- Fully Compliant with USB Specification v2.0
- Software Runs on Windows 10, Windows 8, and Windows 7 for Both 64-Bit and 32-Bit Versions
- 3.3V ±3% 1-Wire Operating Voltage
- Convenient On-Board Test Points and TDFN Socket
- Evaluation Software Available by Request
- Proven PCB Layout
- Fully Assembled and Tested

DS28C36/DS28E36 EV System

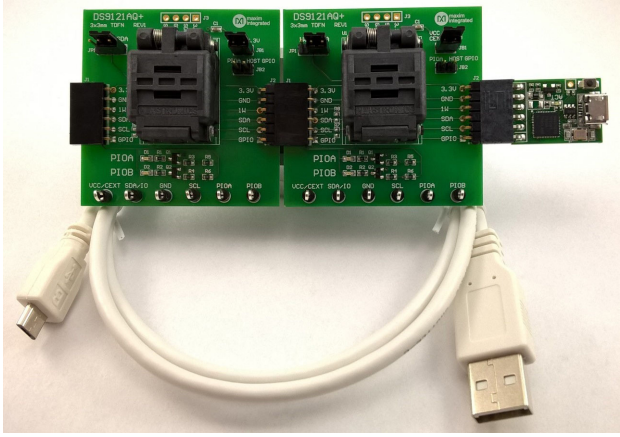


Figure 1. DS28C36EV or DS28E36EV with USB Cable

19-8600; Rev 1; 5/17

maxim integrated™

Quick Start

This section is intended to give the DS28C36/DS28E36 evaluator a list of recommended equipment and instructions on how to set up a Windows-based computer for the evaluation software.

Recommended Equipment

- DS28C36/DS28E36 EV system USB-to-I2C adapter with DS2476 secure coprocessor (included)
- DS9120AQ+ TDFN socket board (included)
- Five DS28C36Q+ or DS28E36Q+ (included respectively)
- Five DS2476Q+ (included)
- USB Type A to Micro-USB 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
- DS28C36 EV system software—if needed, go to **http://support.maximintegrated.com/embeddedsecurity** and fill out the required fields. Enter your request for the DS28C36 EV kit software in the large text box. Then submit the request to receive **DS28C36 EVKIT_REV_1_5_preliminary_051917.zip** or newer version software.

Note: In the following sections, software-related items are identified by **bolding**. Text in bold refers to items directly from the EV system software. Text in **bold and underlined** refers to items from the Windows operating system.

Hardware Setup and Driver Installation Quick Start Procedure

The EV system is fully assembled and tested. The following steps were performed on a Windows 7 PC to set up the DS28C36EVKIT hardware/software:

1) Obtain and unpack the zip of **DS28C36 EVKIT_REV_1_5_preliminary_051917.zip** or newer version.
2) In a file viewer, double click on **DS28C36_Installer.msi** to begin the installation (Figure 2).
3) The Setup Wizard opens. Click on **Next**, as shown in Figure 3.
4) Read and check the box for the license agreement and click on **Next** again to install to the selected folder (Figure 4).

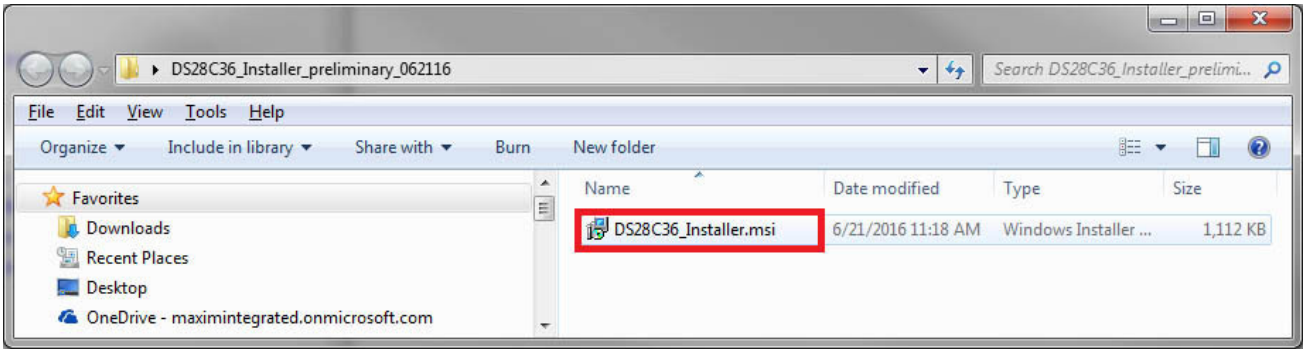


Figure 2. File Viewer

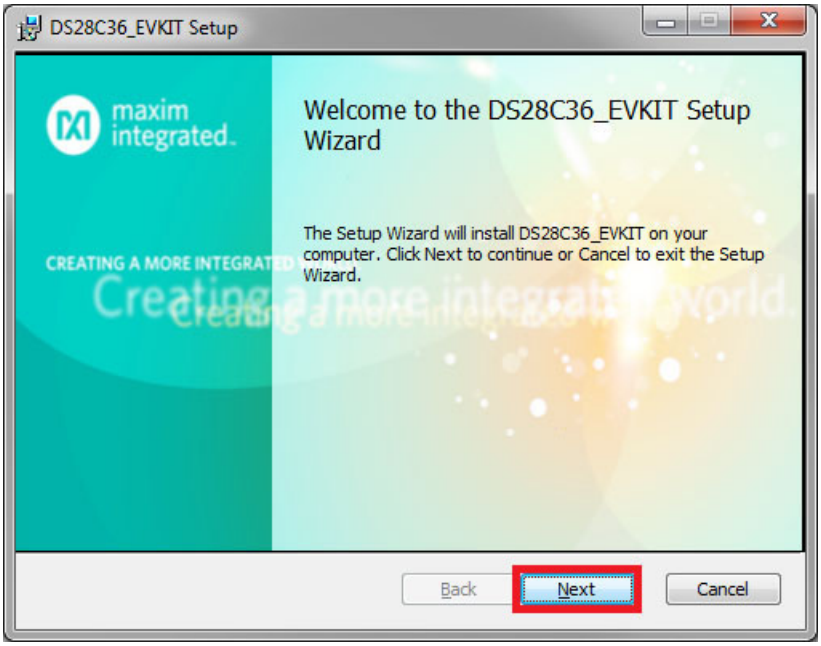


Figure 3. DS28C36 Setup Wizard

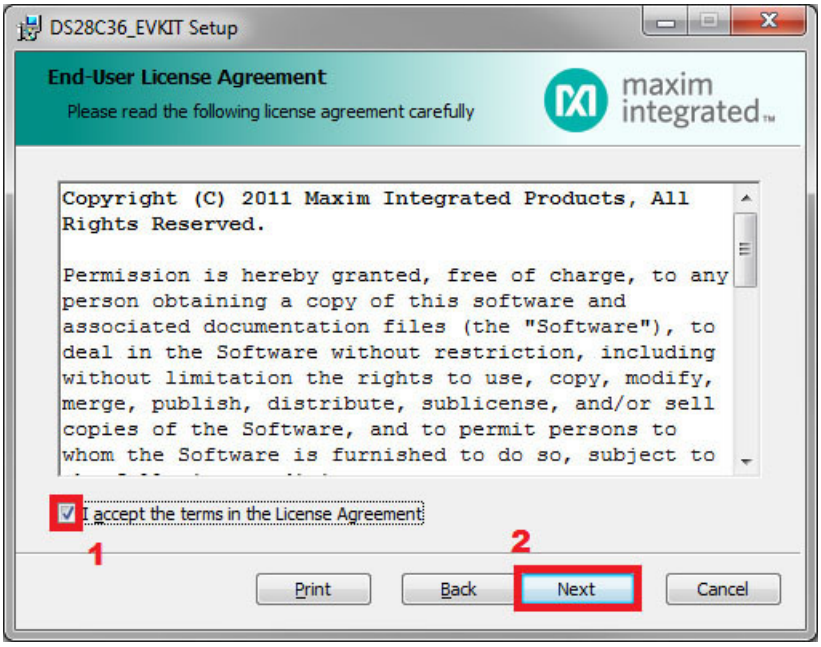


Figure 4. License Agreement Setup Wizard

5) Click the **Next** button to install to the default folder (Figure 5).
6) Unplug all Maxim adapters and click the **Install** button (Figure 6).
7) When the **Windows Security** window appears, click the **Install** button (Figure 7).
8) Click the **Finish** button to exit the Setup Wizard (Figure 8).

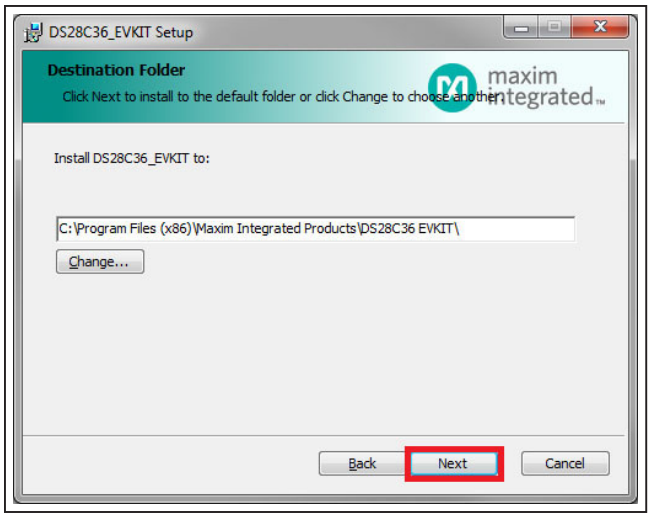


Figure 5. Install Folder Location

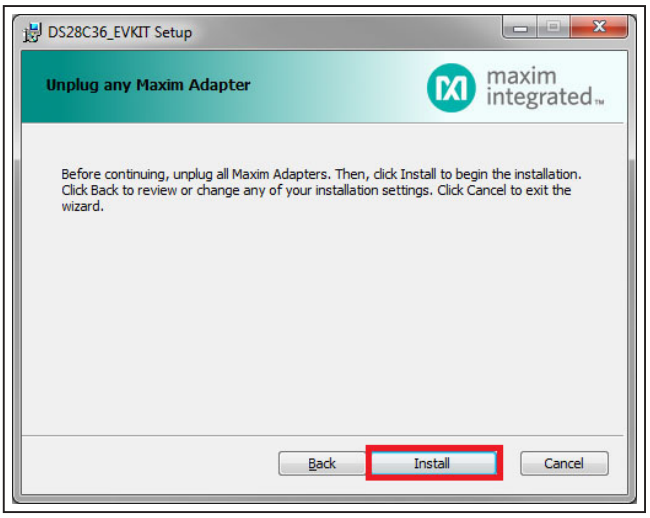


Figure 6. Installation

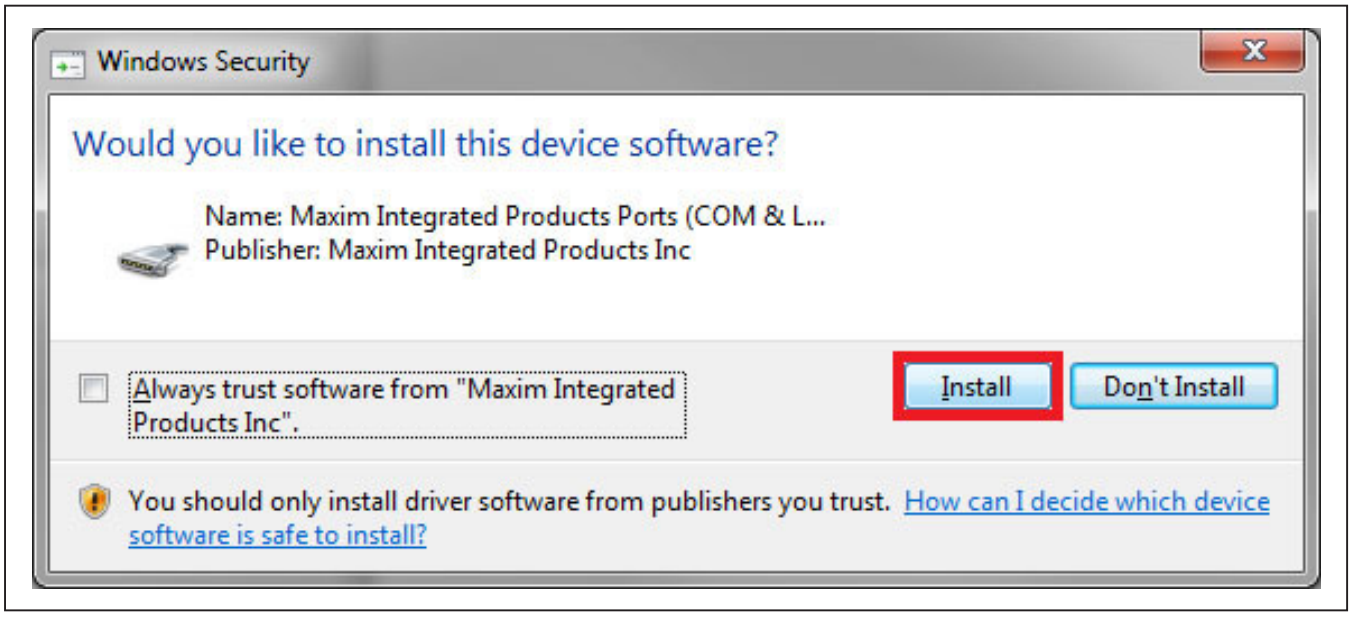


Figure 7. Windows Security Window

9) Plug in the DS9481P-300# to the PC with both DS9120AQ+ socket boards by doing the following:
   a) Open the first burn-in socket and insert a DS2476Q+ into one of the cavities, as shown in Figure 9. **Note:** The plus (+) on the package must be on the opposite side of the marker in the socket.
   b) Open the second burn-in socket and insert a DS28C36Q+ or DS28E36Q+ into one of the cavities, following the same orientation shown in Figure 9.
   c) Close both burn-in sockets.
   d) Connect the first DS9121AQ J2, 6-pin female socket into the DS9481P-300#, 6-pin male plug, as shown in Figure 10.
   e) Connect the second DS9121AQ J2, 6-pin female socket into the 1st DS9121AQ J1, 6-pin male plug. (Figure 10).
   f) For the first socket board with DS2476, configure the jumpers JP1 to use SDA and JB1 to use 3.3V. For the second socket board with DS28C36, configure the jumpers JP1 to use SDA and JB1 to use3.3V. Otherwise with the DS28E36, configure the jumpers to JP1 to use 1W and do not poplulate JB1 (Figure 10).
   g) Plug the DS28C36 EV kit into the PC using a USB Type-A to Micro-USB Type-B cable.

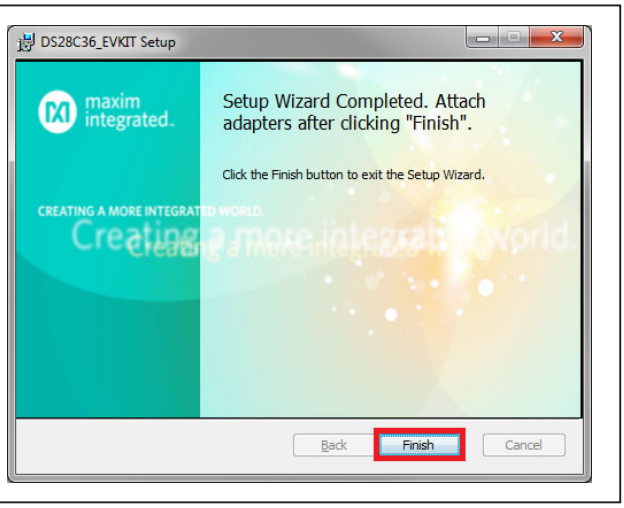


Figure 8. Finish Setup Wizard

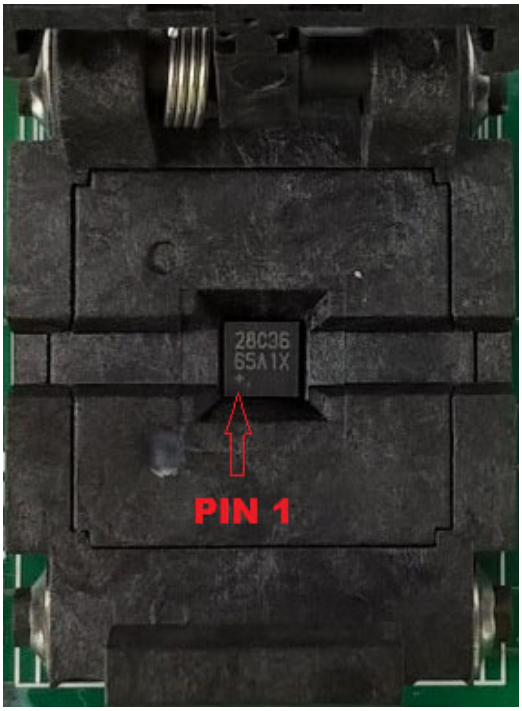


Figure 9. Orientation of the DS28C36, DS28E36, and DS2476 in the Burn-In Socket

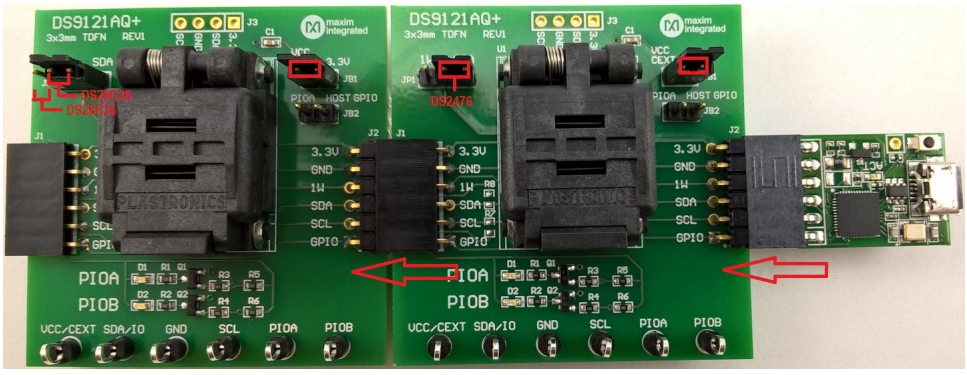


Figure 10. DS9481QA-300 and DS9121AQ

10) The device driver now automatically installs and a pop-up window appears when complete (Figure 11).
11) Open the **DS28C36 EVKIT** from the start menu → **All Programs** → **Maxim Integrated** → **DS28C36 EVKIT**.
12) The DS28C36 EVKIT program opens automatically (Figure 13), finding the COM port and the DS28C36/DS28E36/DS2476.

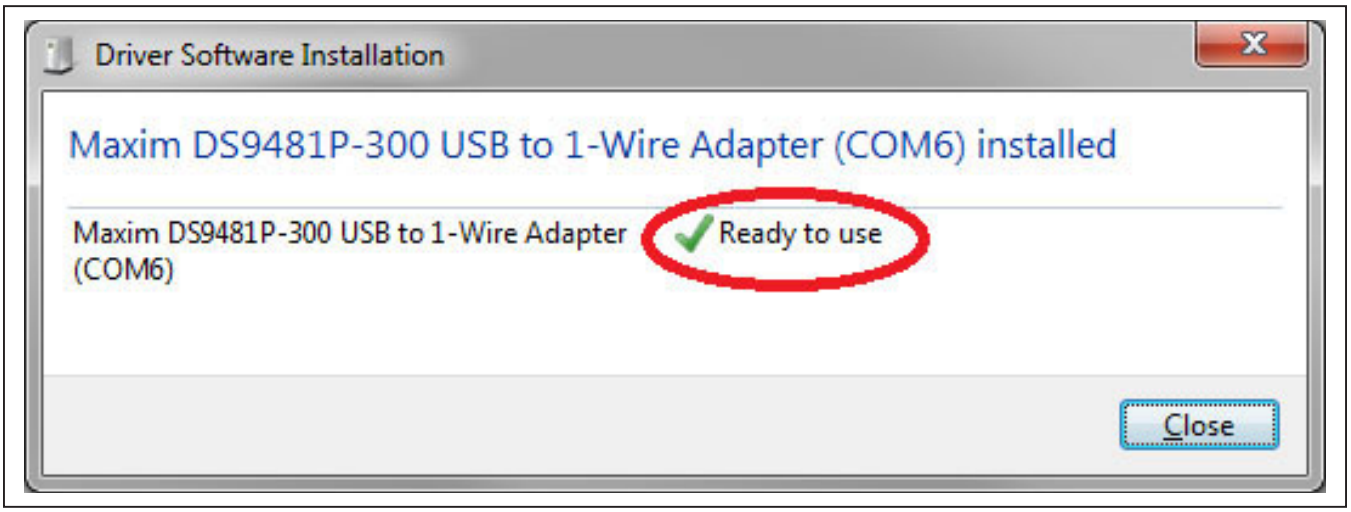


Figure 11. Driver Software Installation Notice

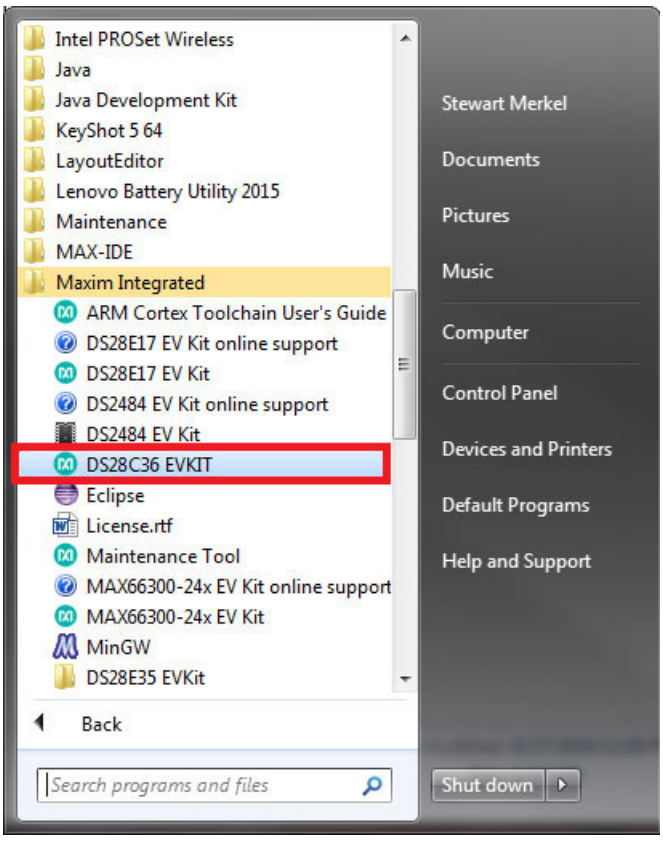


Figure 12. Open DS28C36 EVKIT Program

Detailed Description of Software

The DS28C36 evaluation program user interface (Figure 13) has four tabs, **General Commands**, **SHA2 Commands**, **ECDSA Commands**, and **Other Coprocessor Commands**. The **Setup** section is used to make the device selections that apply to the **General Commands**, **SHA2 Commands**, **ECDSA Commands**, and **Other Coprocessor Commands** tabs. Here is a summary of the function of each tab:

- **General Commands** is used as the main tool to evaluate the DS28C36/DS28E36/DS2476 general functions to write or read from the user memory pages, crypto-related memory pages, decrement counter, RNG, and protection registers.
- **SHA2 Commands** is used to evaluate the DS28C36/DS28E36/DS2476 symmetric (SHA-256) security function commands.
- **ECDSA Commands** is used to evaluate the DS28C36/DS28E36/DS2476 integrated asymmetric (ECC-P256) security function commands.
- **Other Coprocessor Commands** is used to evaluate the DS2476 coprocessor that computes any required HMACs or ECDSA signatures with its additional command set to do any operations on the DS28C36/DS28E36. **Note:** Grayed out when DS28C36 or DS28E36 is selected.

All tabs include a communications **Log** area consisting of an I²C Log or 1-Wire Log output.

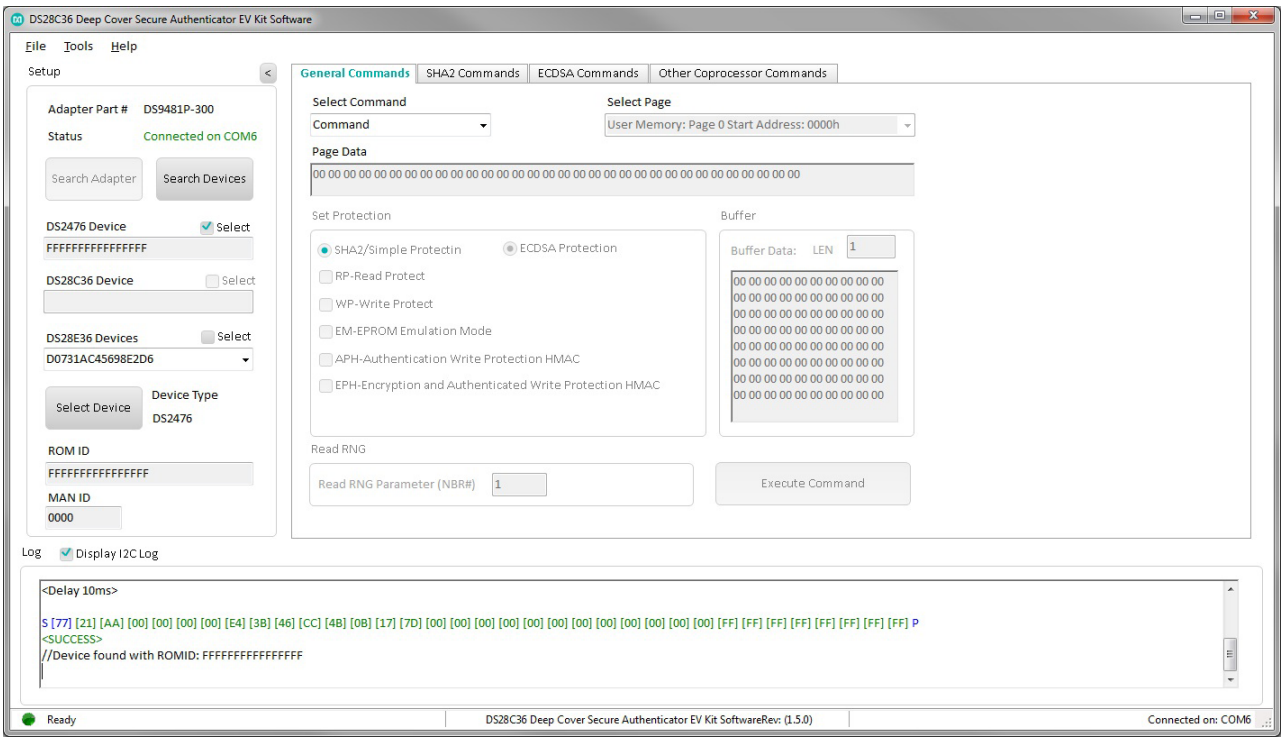


Figure 13. DS28C36 EVKIT Program (Default View Upon Opening)

Setup

The **Setup** area selects devices for control from the tabs (Figure 14) and Table 1 explains the elements of the **Setup** area.

Tutorial of Feature Authentication with ECDSA

This tutorial applies to the *Application Examples* section in the DS28C36 data sheet, which includes the *Feature Authentication with ECDSA Setup* and *Usage (Read Feature)* sections. This tutorial is also comparable to the *Application Example* section in the DS28E36 Security Guide that includes the Feature Authentication with ECSA , but with the DS28E36 device selected instead. The start of this tutorial begins right after Figure 13.

Setup

Use this section to set up the DS28C36. **Note:** This is typically done during manufacturing. Likewise, DS28E36 can be substituted for DS28E36 for the subsequent steps in this section.

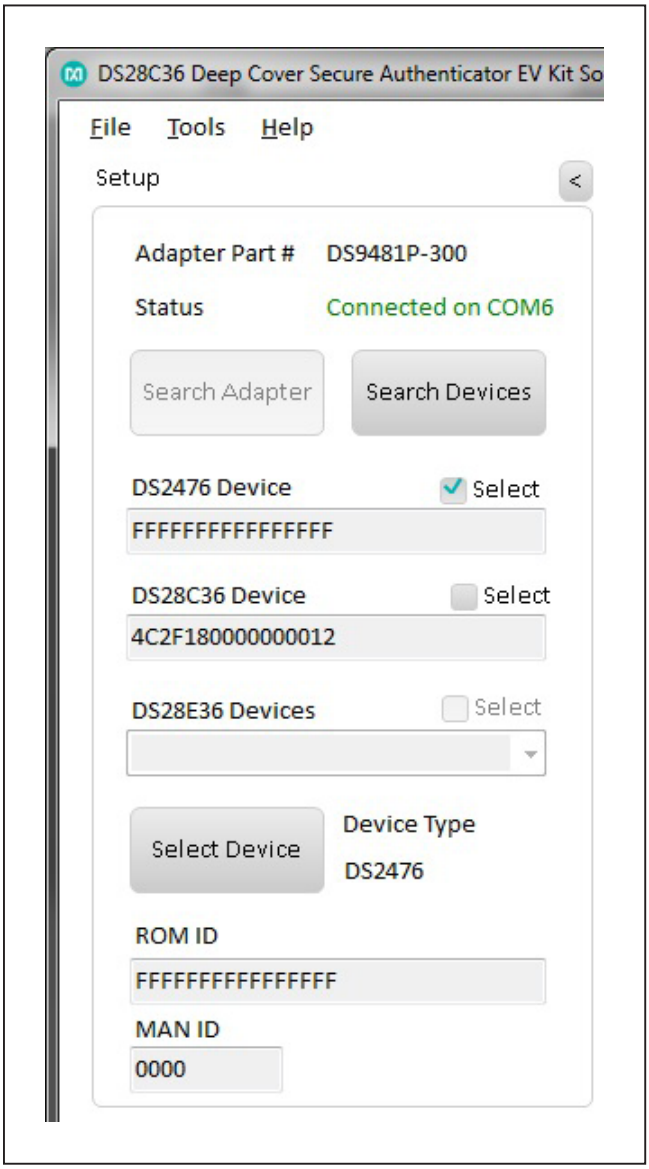


Figure 14. Setup Area

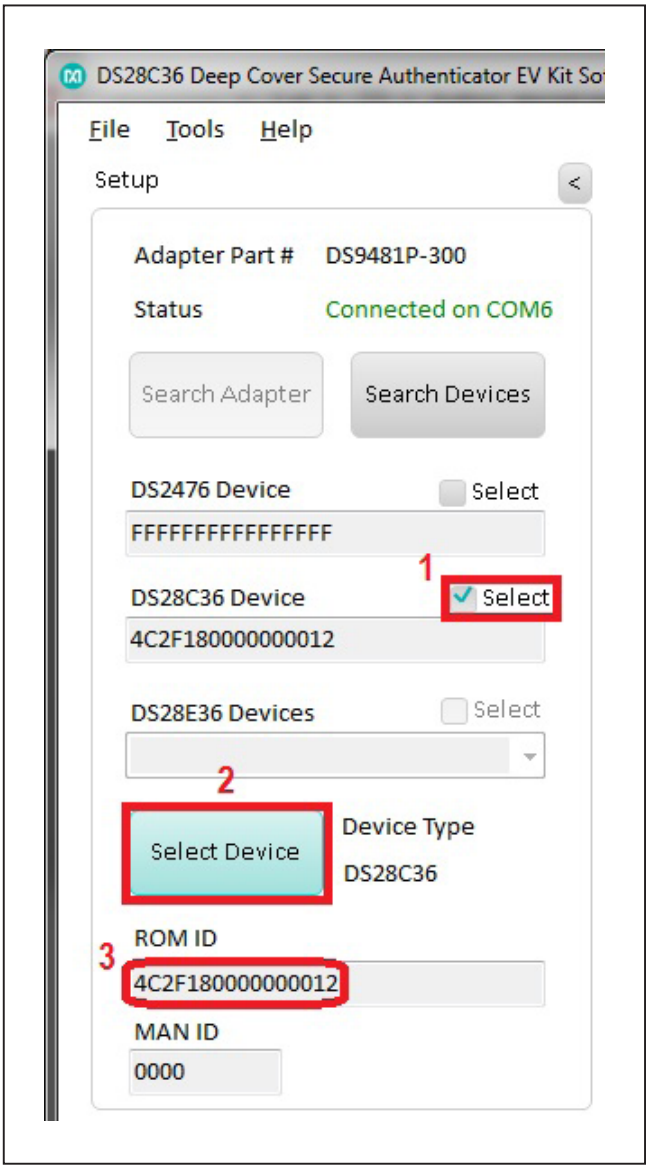


Figure 15. Selecting DS28C36 in the Setup Area

Table 1. Setup Tab, 1-Wire Adapter Section

ELEMENT NAME (TYPE)	PURPOSE	USAGE, SETTING
Status	Port type selection.	**Setting:** Must read USB (COM).
Adapter Part # (Display)	Shows the adapter type needed for the EV kit.	**Usage:** Only allows for DS9481P-300 adapter.
Search Adapter (Action button)	Searches for any connected DS9481P-300 needed for the EV kit.	**Usage:** If no adapter was found after opening the GUI, this button can be used to search and find the DS9481P-300 adapter when connected.
Search Devices (Action button)	Searches for any devices that are connected.	**Usage:** Finds any devices connected.
DS28C36 Device (Display)	Displays the ROM ID of a DS28C36 if connected.	**Usage:** Displays the ROM ID that is selectable for control by the tabs.
DS28C36 Device; Select (Checkbox)	Enables the DS28C36 to be selectable if present.	**Setting:** Checked if this is the only device connected; otherwise, check it to be selectable.
DS28E36 Device (Display)	Displays the ROM ID of a DS28E36 if connected.	**Usage:** Displays the ROM ID that is selectable for control by the tabs.
DS28E36 Device; Select (Checkbox)	Enables the DS28E36 to be selectable if present.	**Setting:** Checked if this is the only device connected; otherwise, check it to be selected.
DS2476 Device (Display)	Displays the ROM ID of a DS2476 if connected.	**Usage:** Displays the ROM ID that is selectable for control by the tabs.
DS2476 Device; Select (Checkbox)	Enables the DS2476 to be selectable if present.	**Setting:** Checked if this is the only device connected. Otherwise, check it to be selectable.
Select Device (Action button)	Selects the selectable device.	**Usage:** This device is chosen by a checked box or drop-down list to be controlled by the tabs (e.g., General Commands, SHA2 Commands, etc.).
Device Type (Display)	Reports the device selected.	**Setting:** Shows the active device for all the tabs.
ROM ID (Display)	Reports the ROM ID in the display box.	**Setting:** Shows the active ROM ID being used by all the tabs.
MAN ID (Display	Reports the MAN ID in the display box.	**Setting:** Shows the active MAN ID being used by all the tabs.

1) Select device DS28C36 by checking its **Select** box, clicking the **Select Device** button, and then observing that the **ROM ID** field is updating with the DS28C36's ROM ID value (Figure 15). Note: The 1-Wire version of the DS28C36 (or DS28E36) can be used by selecting it instead.
2) This step performs the **Generate ECC-256 Key Pair (A)** command with lock (write protection) disabled for the DS28C36. In an actual application, the lock should be enabled and can be done here by checking **Lock (WP) Key Pair Pages**. For demonstration, it is better not to lock the part until the engineer gains enough familiarity with the system. First, select the **ECDSA Commands** tab (affects DS28C36), and then from the drop-down list, select the **Generate ECC-256 Key Pair** command (Figure 16), followed by clicking on the **Execute Command** button. Observe the **Public Key AX** and **AY** fields are populated with the new key pair. Take note that the **Private Key A** displays just FFs, since its true value is hidden in the DS28C36.
3) To create and write the certificate, select the **Tools** tab from the drop-down list and then **Authentication Setup** (Figure 17).

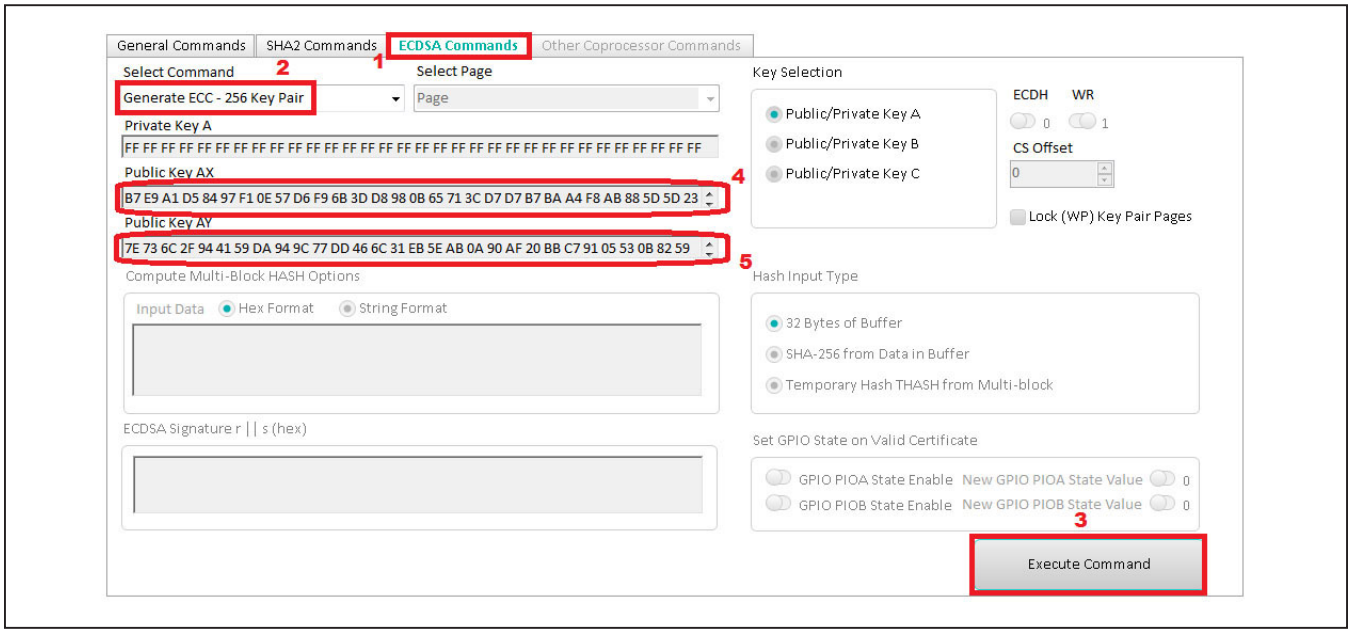


Figure 16. Perform Generate ECC-256 Key Pair for DS28C36

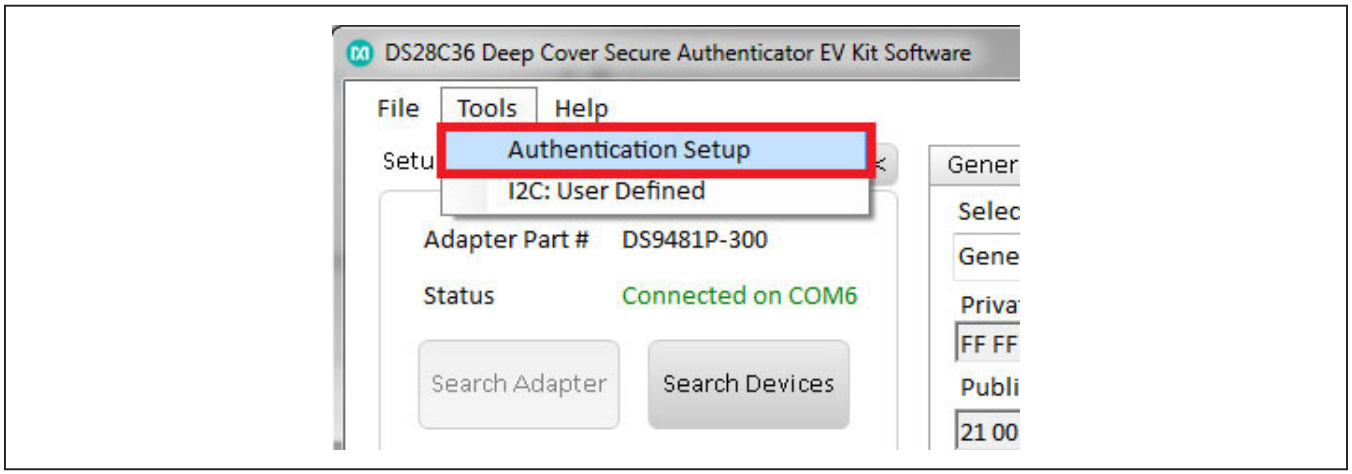


Figure 17. Select Authentication Setup

Observe the ingredient fields in Figure 18 that previously was read using a **Read Memory** command for Public Key Ax/Ay (read during Step 2) and the **ROM ID/MAN ID** (read automatically on startup of the GUI).

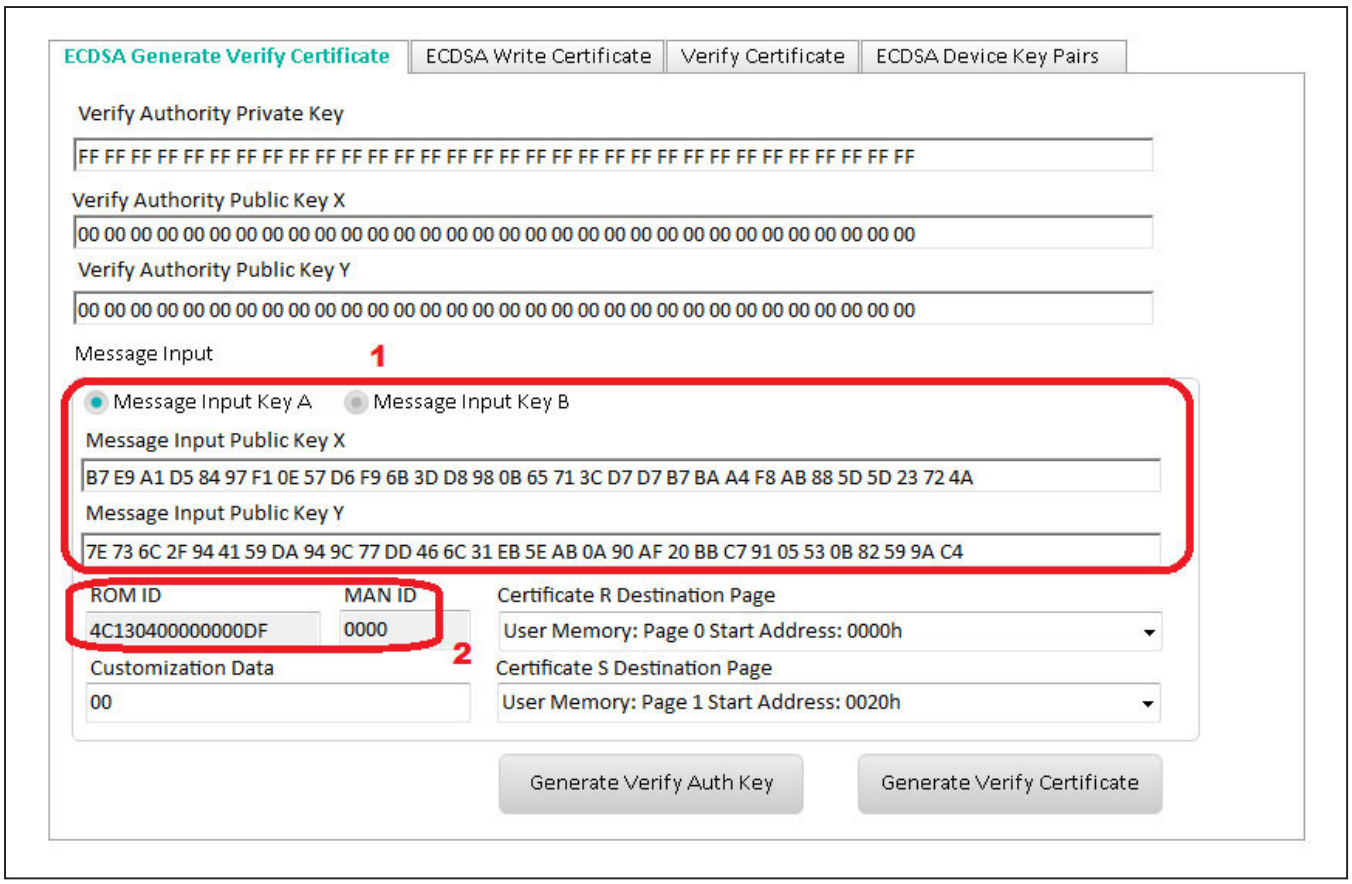


Figure 18. Observing Previous Read Ingredients

Generate the verify authority key by clicking on the **Generate Verify Auth Key** button and observe the generated verify authority key pair (Figure 19). Note the **Verify Authority Private Key** is visible, but should never be made public, as it can be used to generate other certificates. Set the **Certificate R/S Destination Pages** to **User Memory** pages 4 and 5. Now generate and write the certificate by clicking on the **Generate Verify Certificate** button. Note the **Log** shows the actual certificate R and S values created by the verify authority private key and what pages it wrote, too. Due to the different ingredients included to make the signature certificate, a link forms between the DS28C36 device Public Key AX/AY and Verify Authority Key pair. This provides the necessary ingredients needed at later time of read authentication to verify that the DS28C36 is part of the system. Also take note that after writing the certificate to the pages of DS28C36, the Set Page Protection command would usually set the write protect (WP), but this is skipped here since this is for demonstration only.

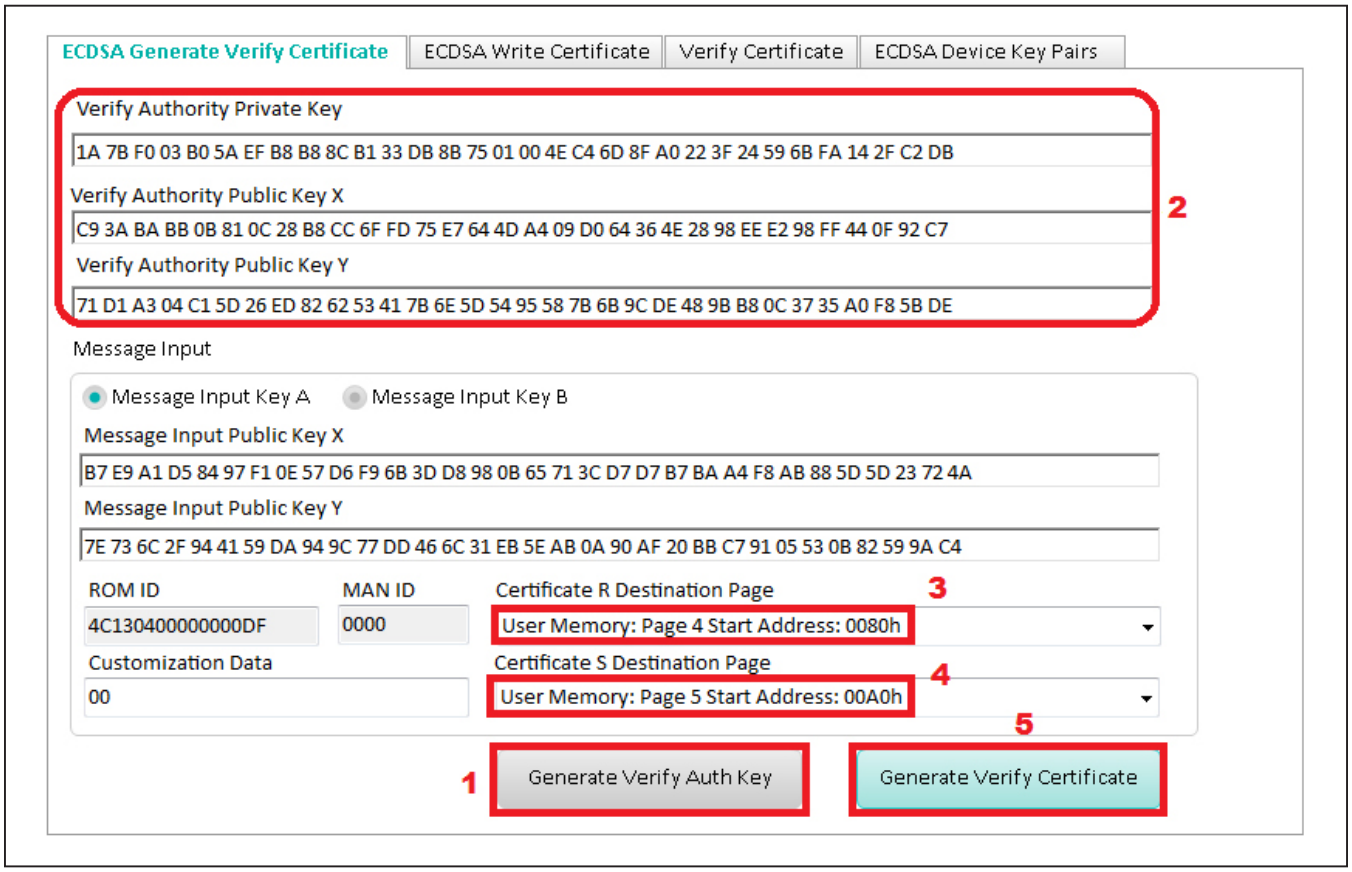


Figure 19. Generating and Writing the Certificate to DS28C36

4) Perform the Write Memory on public key C with the write authority public key per Figure 20a. Select the **ECDSA Write Certificate** tab then the **Generate Write Auth ECC Keys**. Note **Write Authority Key Pair** fields fill with their respective hex values and the **Write Authority Private Key** should be kept secret.

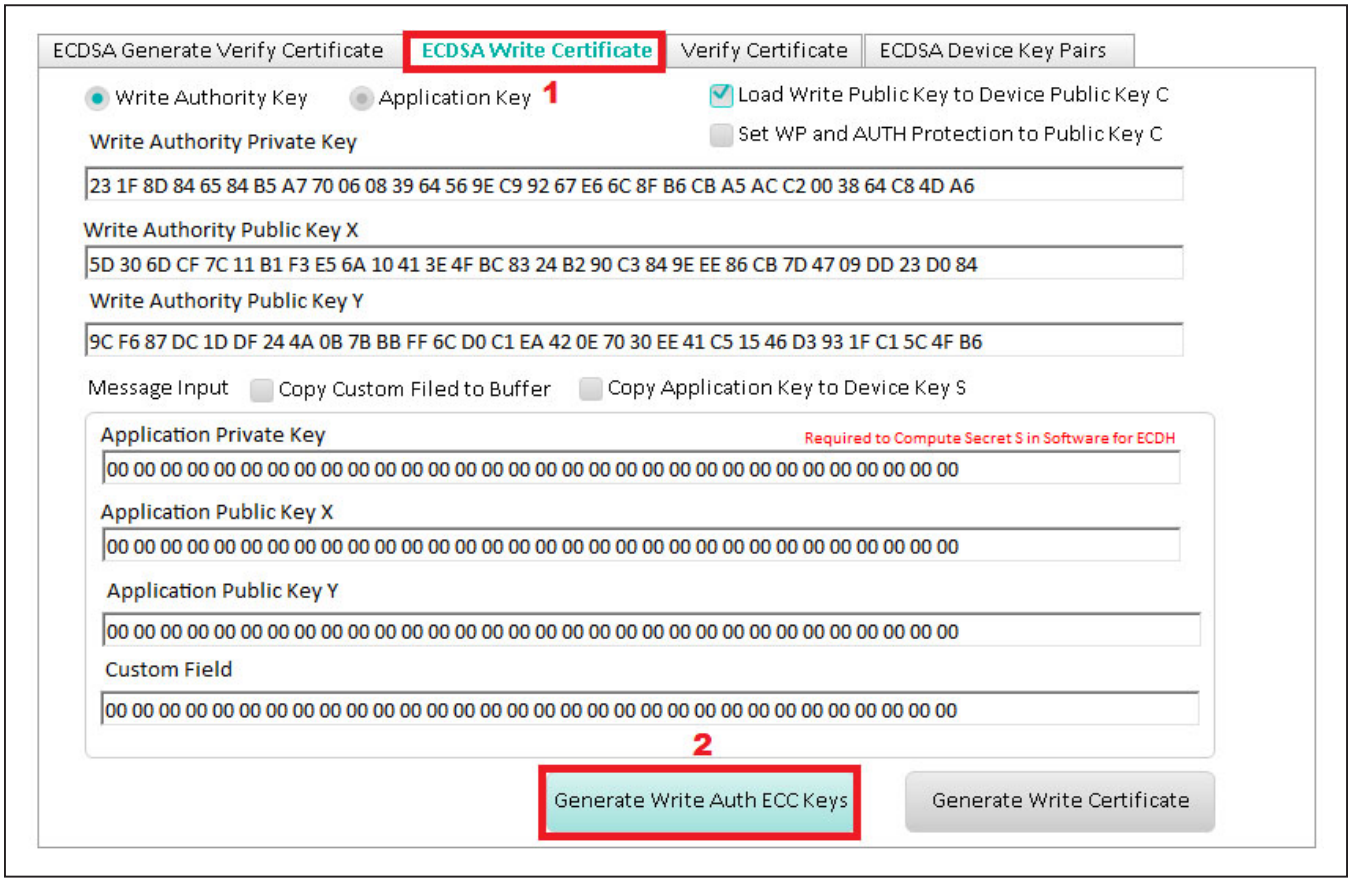


Figure 20a. Generate Write Authority ECC Key Pair

Next, click on the **Load Write Public Key to Device Public Key C**, **Copy Custom Filed to Buffer**, **Copy Application Key to Device Key S** checkbox and then click on the **Generate Application ECC Public Keys**. Now that the application key pair is generated, write the certificate by clicking on the **Generate Write Certificate** button (Figure 20b). Take note that if this was for production and not just demonstration purposes, then clicking on the **Set WP and AUTH Protection to Public Key C** checkbox would also need to be done.

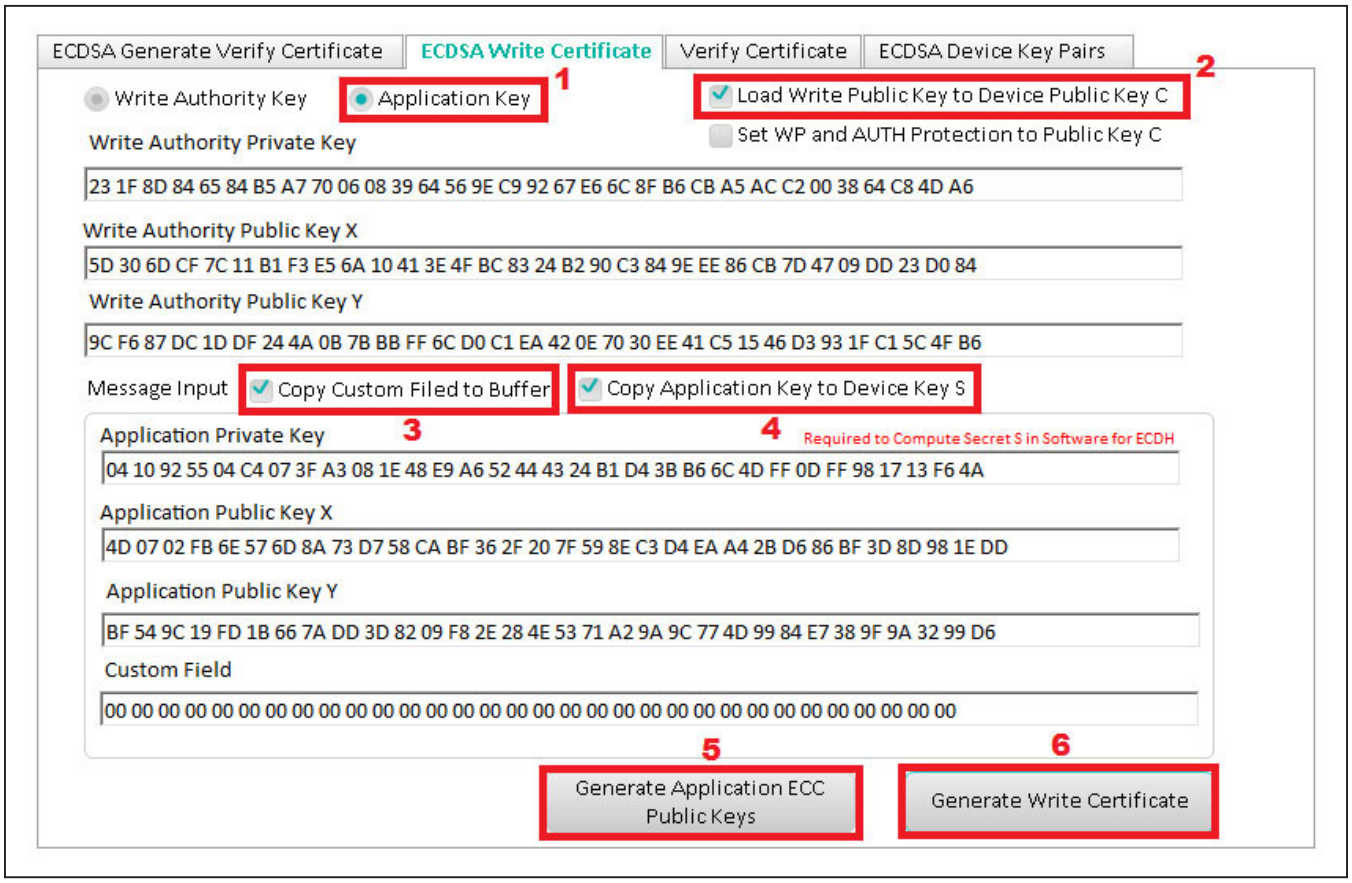


Figure 20b. Generate and Write the Certificate

Lastly, be sure to save the Certificate R/S from the **Log** window in notepad in case of power cycling the DS28C36, as is necessary later on during the **Usage (Write Feature)** section. Close the **Authentication Setup** window.

5) The desired features can now be set in a page of user memory (Figure 21). Select the **General Commands** tab from the **Select Command** drop-down list and select **Write Memory**. From the **Select Page** drop-down list, choose **User Memory: Page 14 Start Address: 01E0h** and fill in the desired **Page Data**. Finally, click on the **Execute Command** button. Note the **Log** should display **<SUCCESS>** at the end with the data just written.

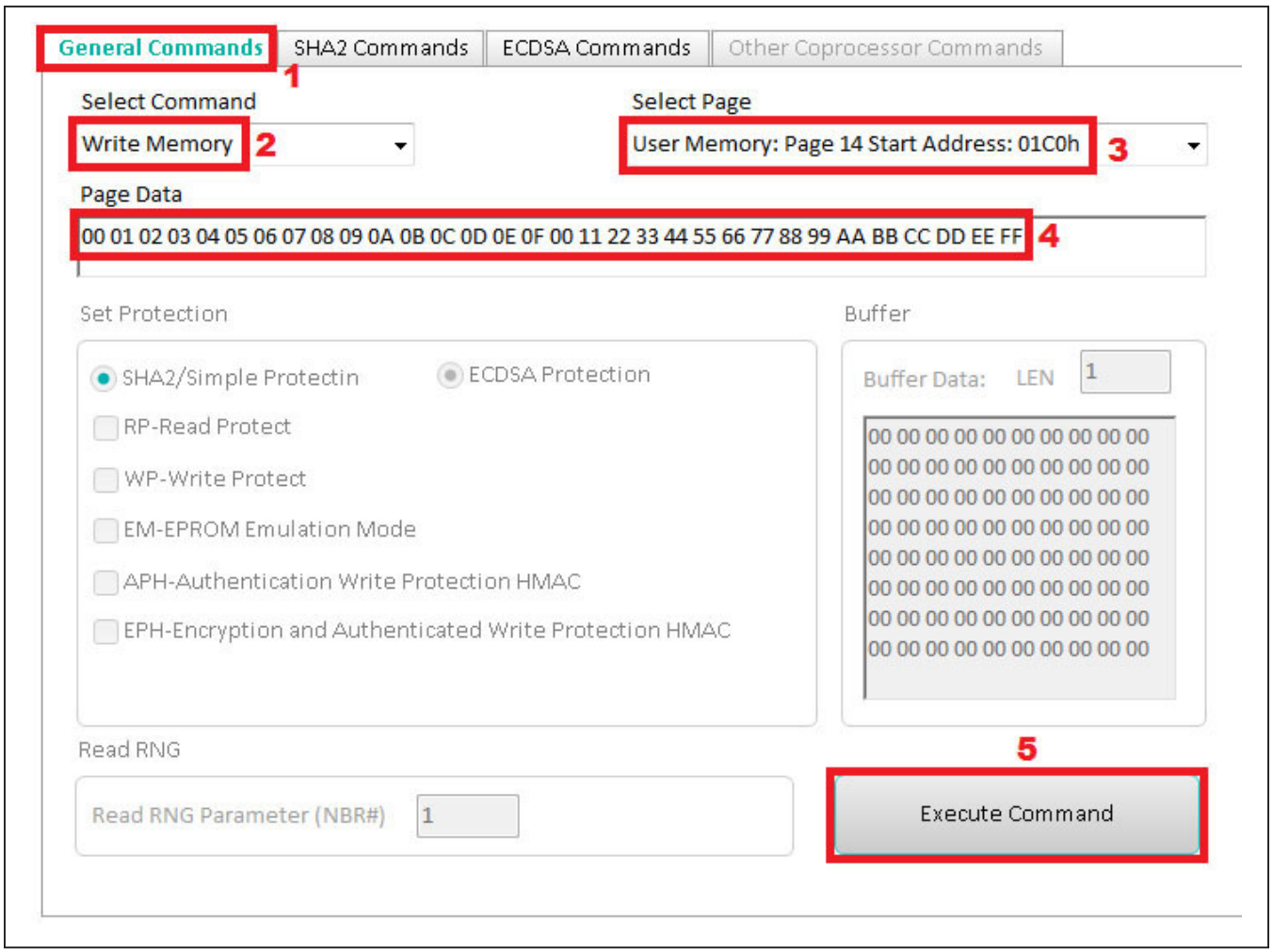


Figure 21. Write Memory Command to Page 14 with Feature Data

6) Perform **Set Page Protection** to set ECW on feature page 14 (Figure 22). From the **Select Command** drop-down list, select **Set Page Protection**. From the **Select Page** drop-down list, choose **User Memory: Page 14 Start Address: 01E0h**. In the **Set Protection** area, click on the **ECDSA Protection** radio button, and finally click on the **Execute Command** button. **Note:** A pop-up window appears with the following message: **The page protection is set to: ECW and it is irreversible. Do you want to continue?** Click **Yes** to demonstrate the write authentication feature. At the end, the **Log** should displays **<SUCCESS>**.

7) The setup for demonstration purposes is now complete for both the read authentication feature and the write authentication feature. However, keep in mind that in the real factory programming, it would be important to also write random data to all unused keys and secrets and set WP protection on each.

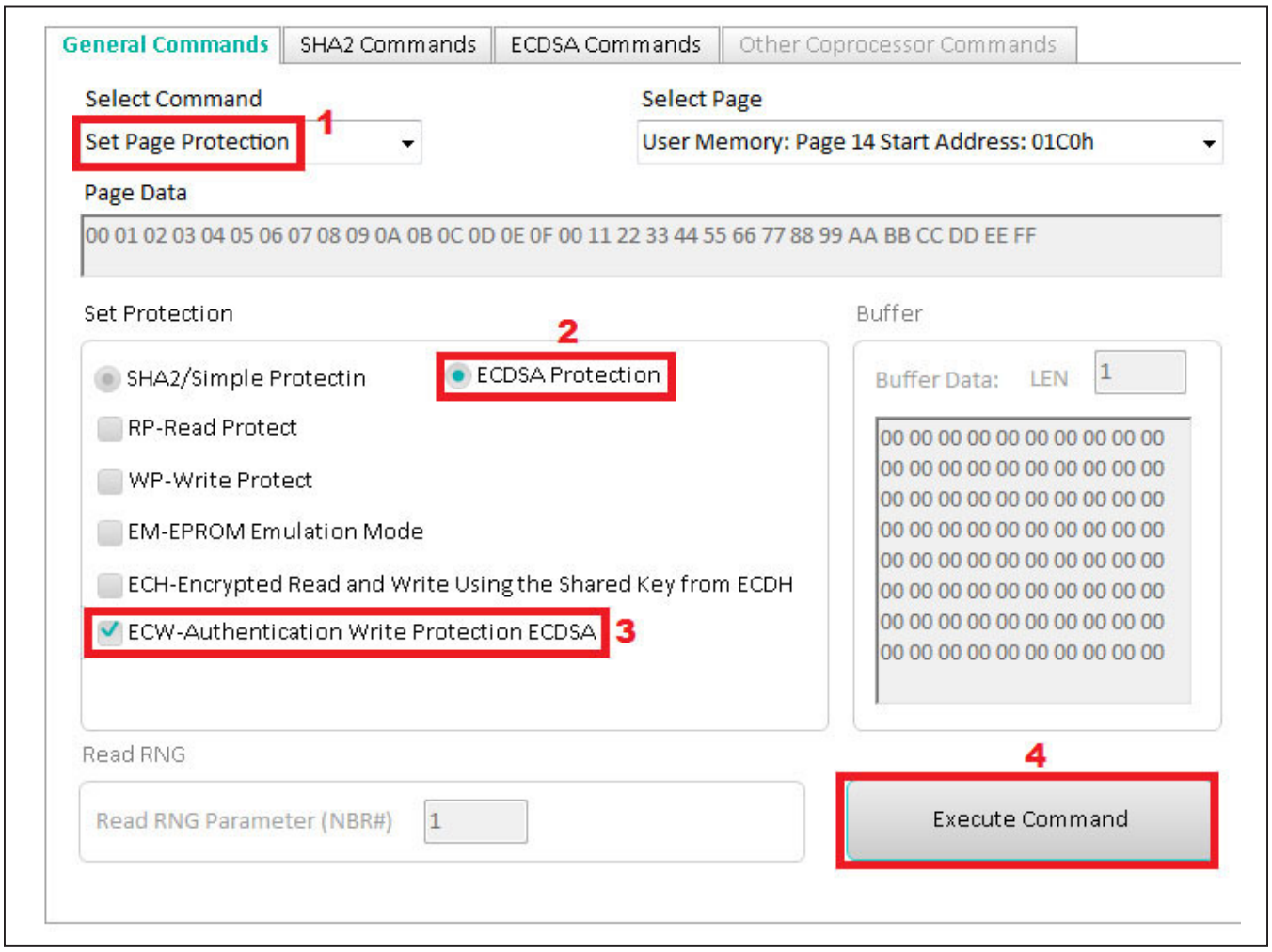


Figure 22. Set Page Protection Command to Page 14 with Feature Data

Usage (Read Feature)

Follow these steps to perform a usage example of reading a feature page and authenticating with the DS28C36 and DS2476. **Note:** The DS28E36 can be substituted for the DS28C36 for the subsequent steps in this section.

1) If not already done, select device DS28C36 by checking its **Select** box, then clicking the **Select Device** button. Observe that the **ROM ID** field is updating with DS28C36's ROM ID value (Figure 15).

2) If not already done, perform **Read Memory** on device public key AX per Figure 23. Select the **General Commands** tab. From the **Select Command** drop-down list, choose **Read Memory**, from the **Select Page** drop-down list, choose **Page 16**, **Pub Key AX** and click on the **Execute Command** button. Confirm the **Page Data** field populates with the correct values.

   Repeat the steps in Figure 23, but change the **Select Page** drop-down list to **Page 17**, **Pub Key AY** to read the device public key AY.

3) Verify the certificate. Go to the **Tools** tab from the drop-down menu and then **Authentication Setup**, as shown in Figure 17.

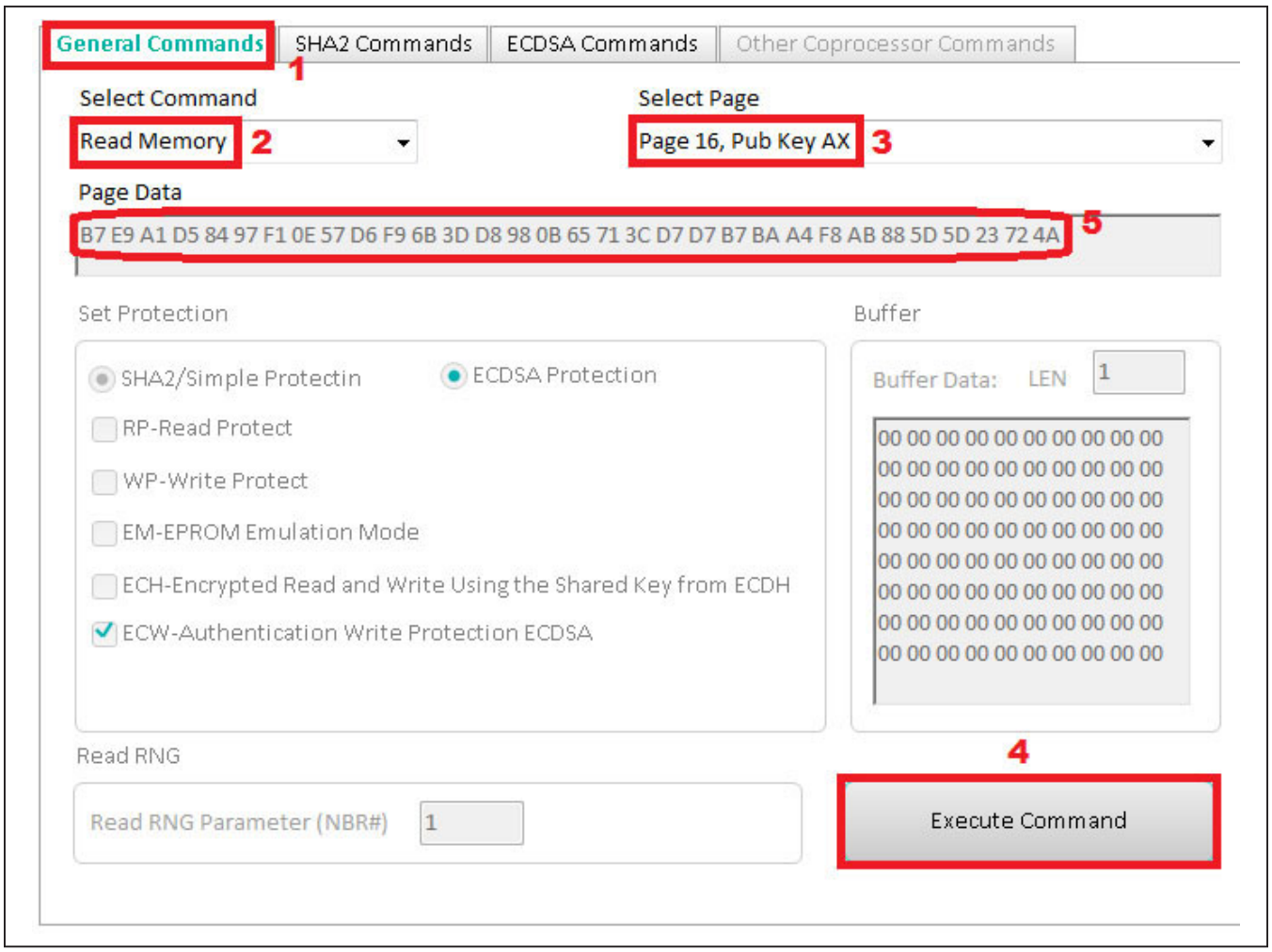


Figure 23. Read Memory Public Key AX of Page 16

4) Perform master verifies certificate for device public key AX/AY, ROM ID, and MANID (Figure 24). Select the **Verify Certificate** tab and check the **Use Coprocessor to Validate Certificate** in the **Message Input**. Choose the **Message Input Key A** radio button, and from the **Certificate R Page** drop-down list, choose **User Memory: Page 4 Start Address: 0080h**. In the **Certificate S Page** drop-down list, choose **User Memory: Page 5 Start Address: 00A0h** for the ingredients. Then click the **Authenticate** button to verify the certificate, confirming that the **Log** displays **Valid ECDSA Signature**. This means the DS28C36 is part of the system, but not yet authentic until it can create a valid digital signature.

   Close the **Authentication Setup** window.

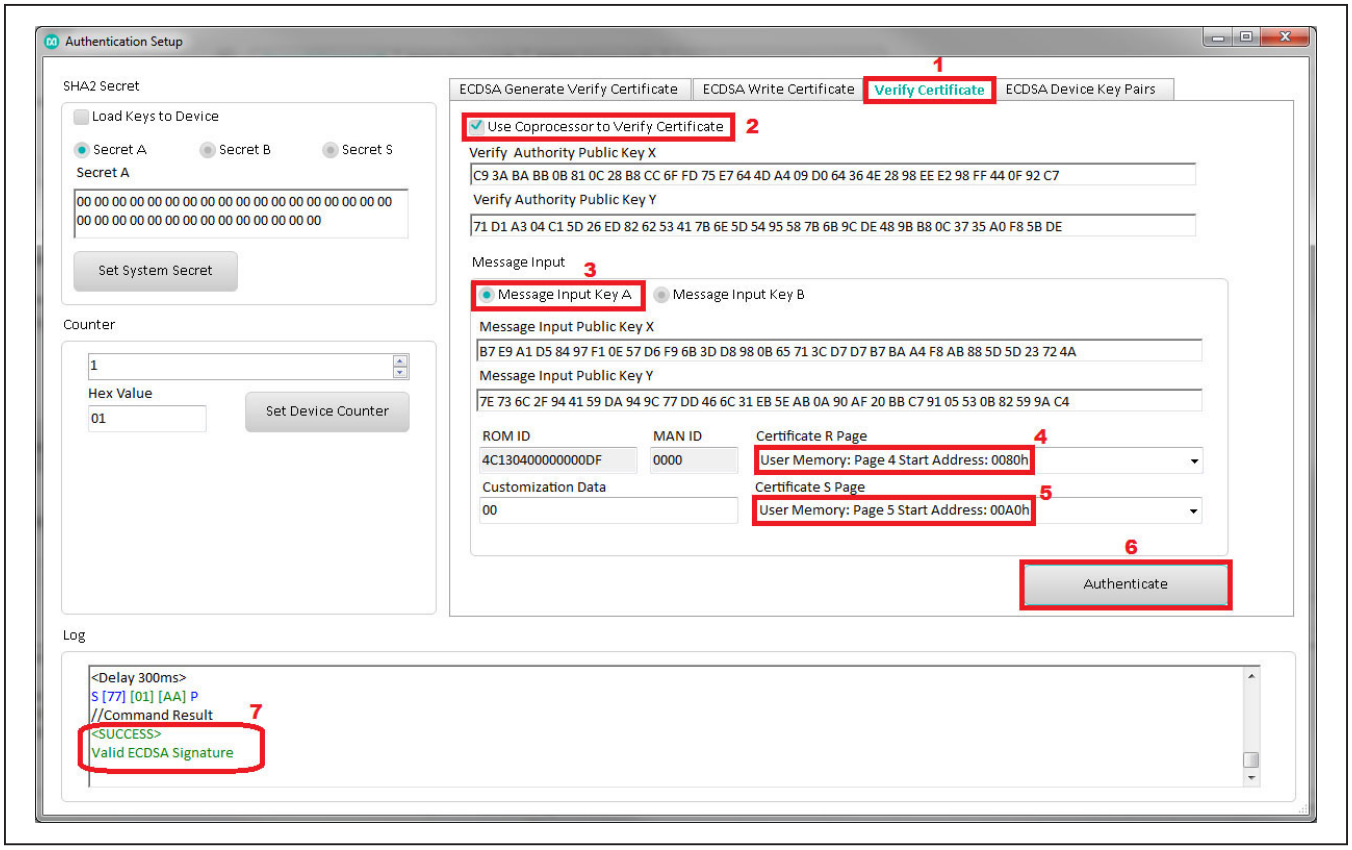


Figure 24. Verify the Certificate using the Coprocessor

5) Perform **Compute and Read Page Authentication** with the ECDSA key set selected on feature page 14 and verify the signature with the coprocessor (Figure 25). Select the **ECDSA Commands** tab, confirm that the **Use Coprocessor** checkbox is selected, and click on **Generate Challenge**. This reads a random number from the coprocessor to be used as the challenge written to the DS28C36 buffer as well. From the **Select Command** drop-down list, choose **Compute and Read Page Authentication**, and from the **Select Page** drop-down list, choose **User Memory: Page 14 Start Address: 01C0h** and confirm that the **Verify Signature Software** checkbox is selected. Clicking the **Execute Command** button computes the **Read Page Authentication** signature from the DS28C36, and then the coprocessor verifies the signature. Confirming that the **Log** displays *Valid ECDSA signature* means the DS28C36 is authentic. **Note:** Both the Verify Certificate in step 4 and the DS28C36's signature had to be verified to be considered authentic. If either verify failed, the DS28C36 would not be authentic.

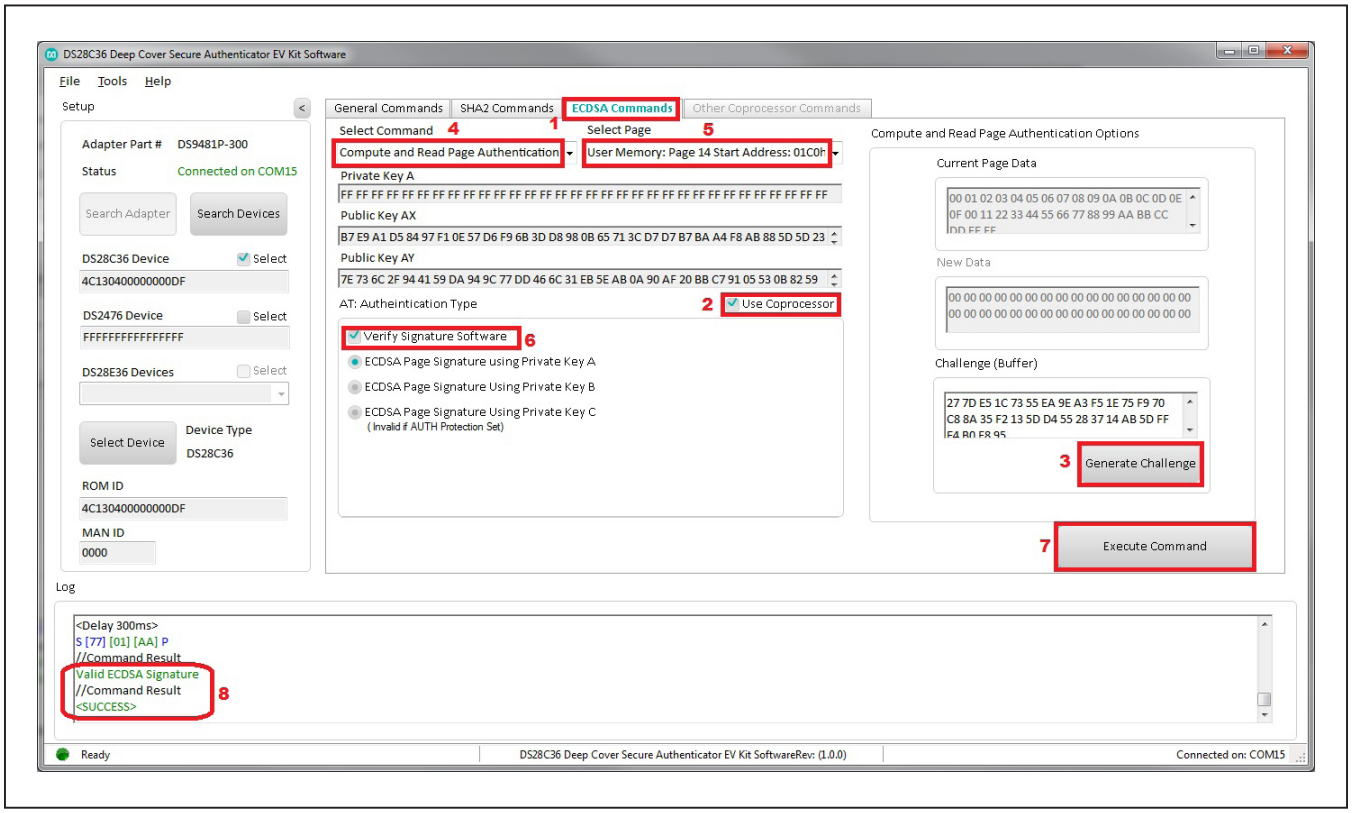


Figure 25. Compute Signature with DS28C36 and Verify Signature using the Coprocessor

Usage (Write Feature)

Follow these steps to perform a usage example of writing a new feature to a page of the DS28C36 with authenticating using the host software.

1) If not already done, select device DS28C36 by checking its **Select** box, then click the **Select Device** button, and observe that the ROM ID field is updating with the DS28C36's **ROM ID** value, as shown in Figure 15.
2) If not already done, perform a **Read Memory** on device public key AX (Figure 23). Select the **General Commands** tab from the **Select Command** drop-down list and choose **Read Memory**. From the **Select Page** drop-down list, choose **Page 16**, **Pub Key AX** and click on the **Execute Command** button. Confirm that the **Page Data** field populates with the correct values.

   Repeat the steps in Figure 23, but change the **Select Page** drop-down list to **Page 17**, **Pub Key AY** to read the device public key AY.
3) Verify the certificate. Go to the **Tools** tab and then **Authentication Setup** (Figure 17).
4) Perform **Read Memory** on user pages 4/5 with device certificate. The Master verifies the certificate for device public key AX/AY (Figure 24). Select the **Verify Certificate** tab, and uncheck the **Use Coprocessor to Validate Certificate**. In the **Message Input** section, click on the **Message Input Key A** radio button, from the **Certificate R Page** drop-down list and choose **User Memory: Page 4 Start Address: 0080h**. In the **Certificate S Page** drop-down list, choose **User Memory: Page 5 Start Address: 00A0h** for the ingredients. Then click the **Authenticate** button to verify the certificate, confirming in the **Log** the text *Valid ECDSA Signature*. This means the DS28C36 is part of the system, but not yet authentic until it can create a valid digital signature. Take note from the output **Log** that the *Verify Authority Public Key* was temporarily written to the Public Key S and the device certificate verified by the coprocessor.

   Close the **Authentication Setup** window.

5) Perform a **Read Memory** on feature page 14 (old data) (Figure 26). Select the **General Commands** tab from the **Select Command** drop-down list, and choose **Read Memory**. From the **Select Page** drop-down list, choose **User Memory: Page 14 Start Address: 01C0h** and click on the **Execute Command** button. Confirm that the **Page Data** field populates with the correct values.

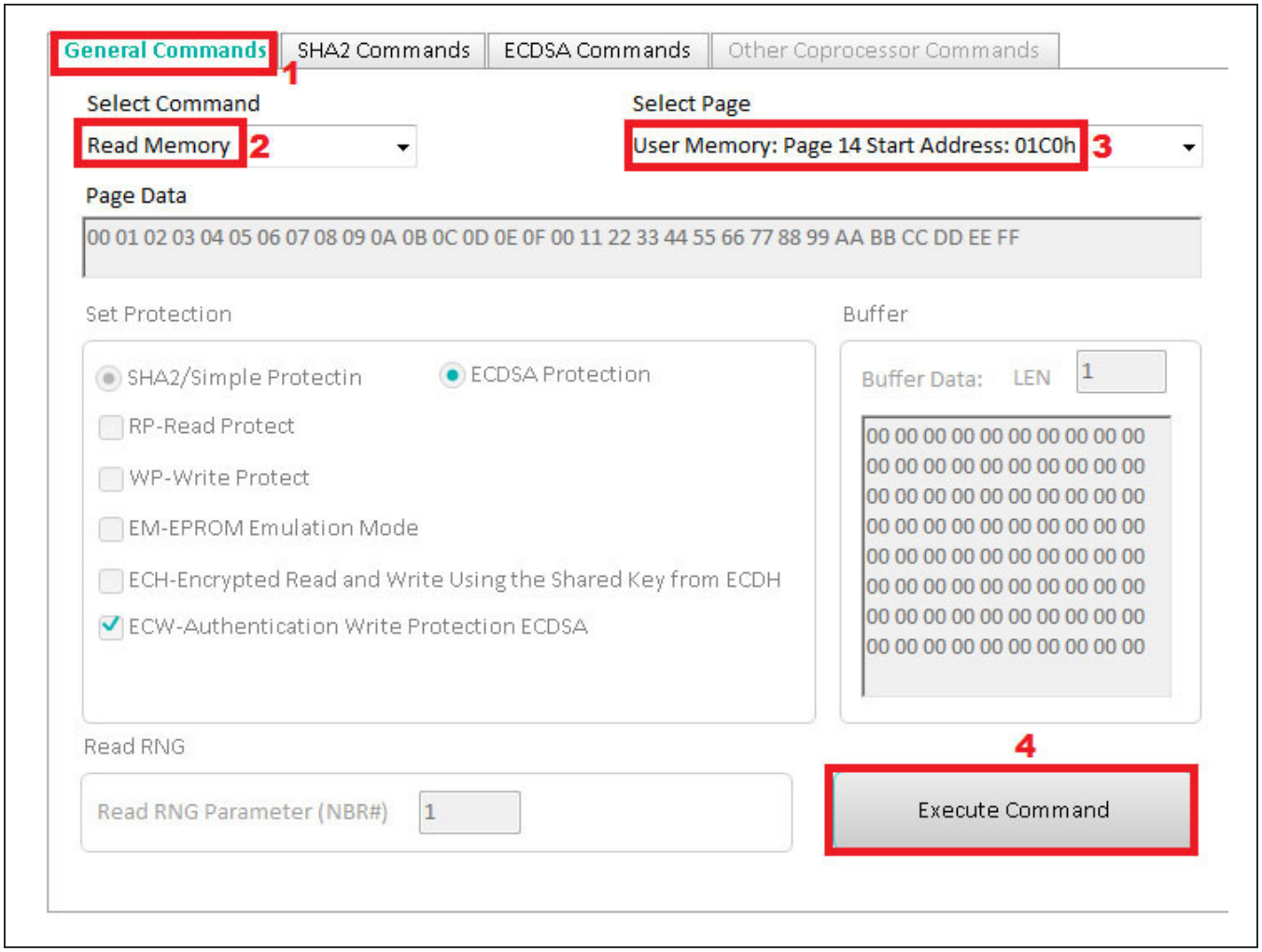


Figure 26. Read Feature Page 14

6) Write the master public key to public key S with the **Write Memory** and perform Authenticate ECDSA Public Key with the Master's public key certificate (this sets W_PUB_KEY to allow public S to authenticate writes), as shown in Figure 27. Select the **ECDSA Commands** tab. From the **Select Command** drop-down list, choose the **Authenticate ECDSA Public Key** command. Choose the **Public/Private Key A** radio button, and set the **CS Offset** field value to 31 (i.e., 32-byte length). Confirm that field values **Public Key AX/AY**, **Public Key SX/SY** and the **Signature/Certificate** are correct. **Note:** If the values are incorrect, then reread or write the correct values using the **General Commands** tab to correct the issue with the **Read/Write Memory** commands. Lastly, click the **Execute Command** button and confirm that the text in the **Log** displays **<SUCCESS>**.

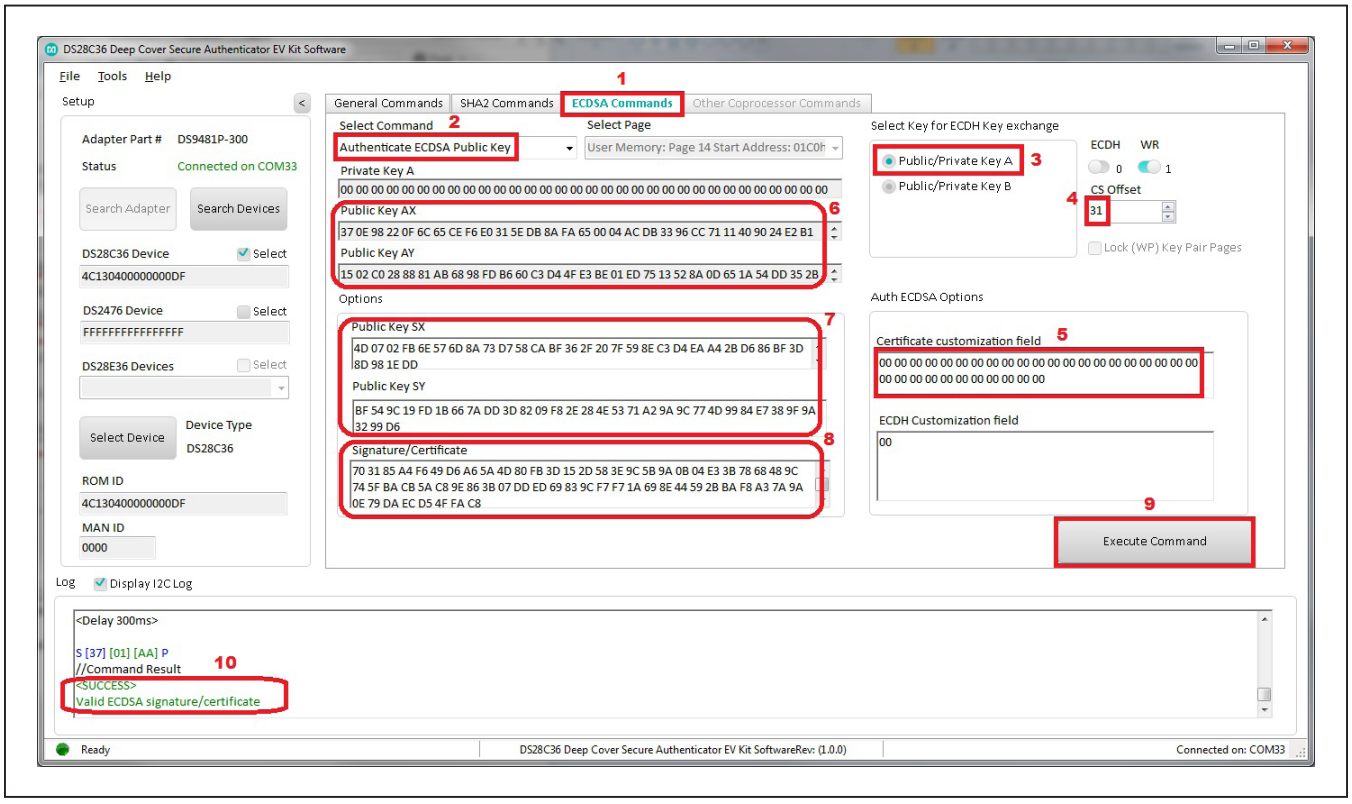


Figure 27. Authenticate ECDSA Public Key with Master's Public Key Certificate

7) Perform Authenticated ECDSA Write Memory with new feature (new data) to page 14 (Figure 28). From the **Select Command** drop-down list, choose the **Authenticated ECDSA Write Memory** command. From the **Select Page** drop-down list, choose **User Memory: Page 14 Start Address: 01C0h** page for new data. Populate the new data fields with the new hex values. Click the **Generate Challenge** button to generate the new challenge and click the **Execute Command** button to run the sequence. Confirm that the new data was written in the **Log** display.

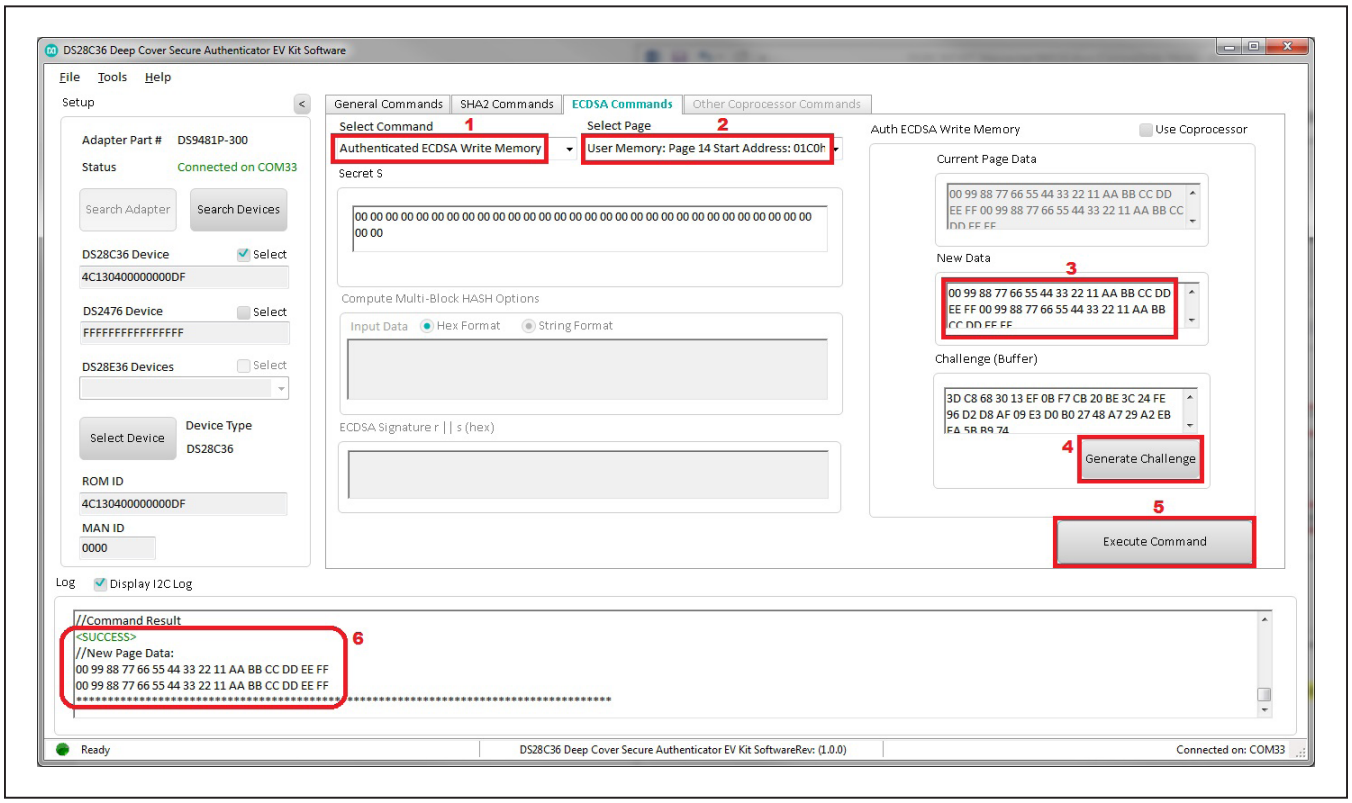


Figure 28. Authenticate ECDSA Write Memory with New Feature (New Data)

8) Perform **Compute and Read Page Authentication** with the ECDSA key set selected on feature page 14 and verify the signature (Figure 29). From the **Select Command** drop-down list, choose **Compute and Read Page Authentication**. From the **Select Page** drop-down list, choose **User Memory: Page 14 Start Address: 01C0h** and confirm that the **Verify Signature Software** checkbox is selected. Uncheck the **Use Coprocessor** checkbox and click on the **Generate Challenge** button. This reads a random number from the host software to be used as the challenge that is written to the DS28C36 buffer as well. Clicking the **Execute Command** button computes the **Read Page Authentication** signature from the DS28C36 and then the host software verifies the signature. Confirming that the **Log** displays *Valid ECDSA Signature* means that the DS28C36 is authentic. **Note:** Both the Verify Certificate in step 4 and the DS28C36's signature had to be verified to be considered authentic. If either verify failed, the DS28C36 would not be authentic.

Detailed Description of Hardware

The DS28C36 EV kit hardware includes a MAXQ1010 microcontroller with USB, DS2476 coprocessor, and a DS9121AQ socket adapter that is made to contain the DS28C36/DS28E36 Secure Authenticators with ECDSA and 8Kb user memory. The MAXQ1010 is loaded with firmware to function as a virtual COM port that bridges UART signaling to I²C or 1-Wire. The DS2476 functions to offload the ECDSA computations to perform signature. The DS28C36 I²C slave or DS28E36 1-Wire slave functions perform ECDSA public-key signatures during an authentication and contains memory space for the necessary ingredients.

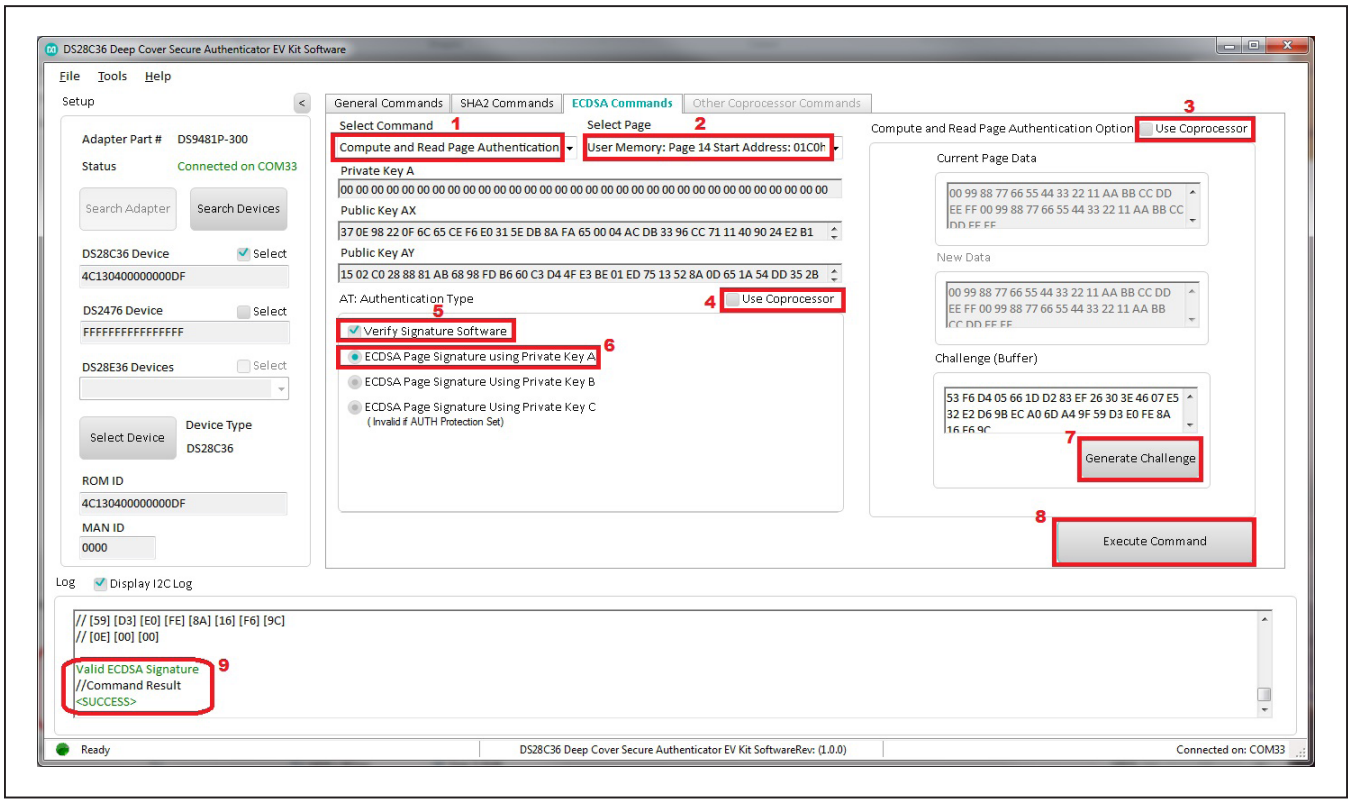


Figure 29. Compute Signature with DS28C36 and Verify with Software

Ordering Information

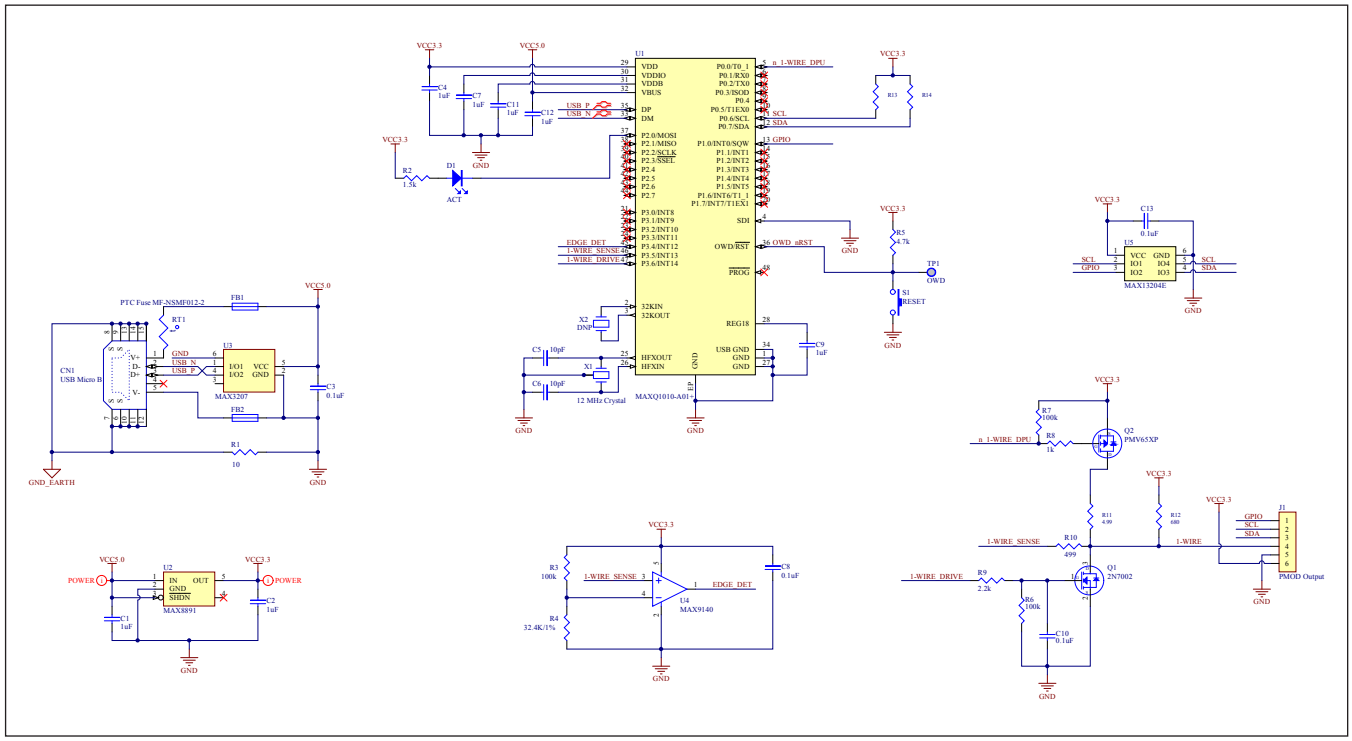
PART	TYPE
DS28C36EVKIT#	EV System
DS28E36EVKIT#	EV System

#Denotes RoHS compliant.

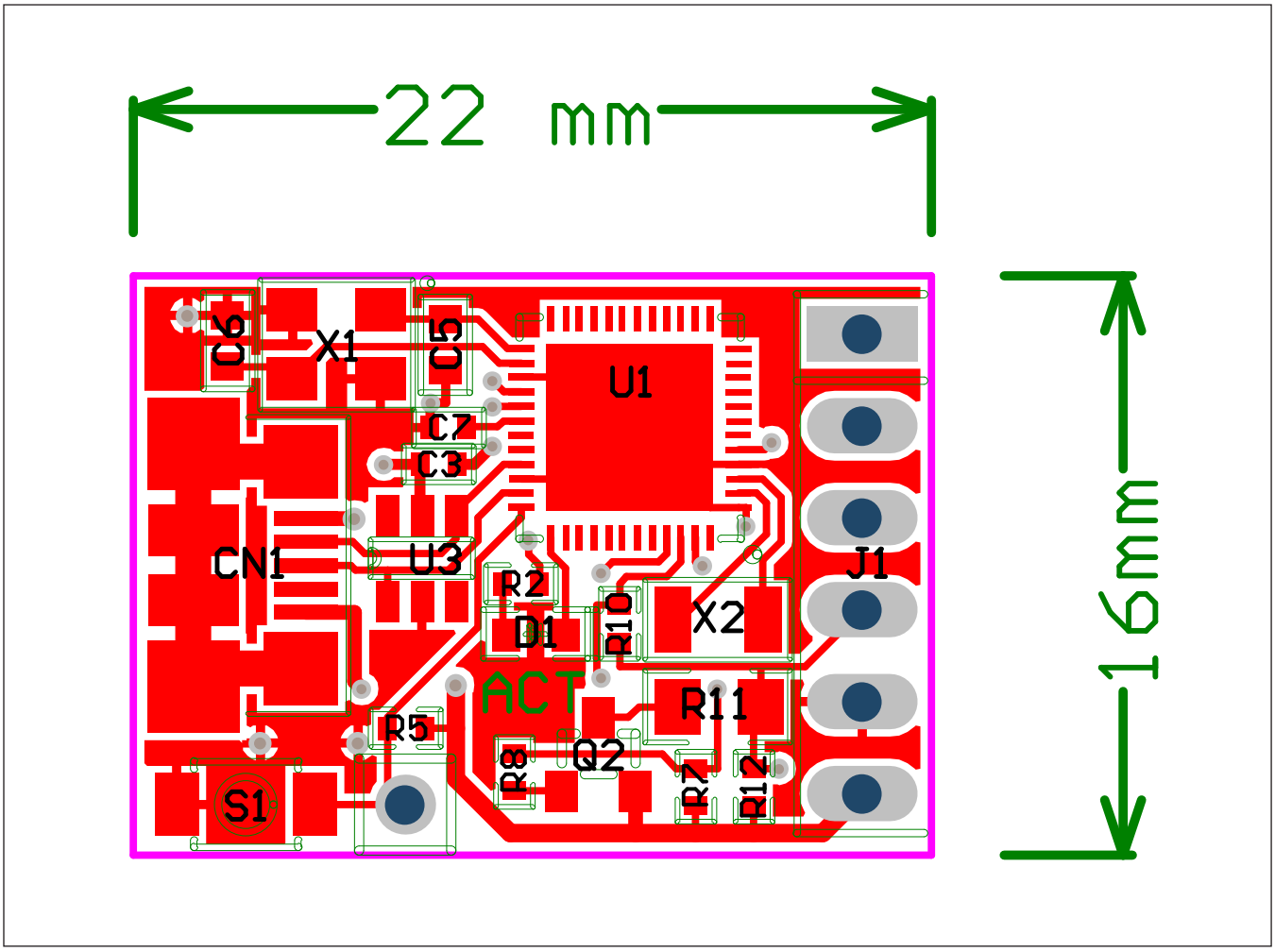
DS9481P-300 Bill of Materials

Designator	Quantity	Description	Manufacturer	Part Number
C1, C2, C4, C7, C9, C11, C12	7	1uF Ceramic Capacitor (0402)	TDK Corporation	C1005X5R0J105M050BB
C3, C8, C13	3	0.1uF Ceramic Capacitor (0402)	TDK Corporation	C1005X5R0J104K050BA
C5, C6	2	10pF Ceramic Capacitor (0603)	TDK Corporation	C1608C0G1H100D080AA
C10	1	10pF Ceramic Capacitor (0402)	MURATA	GRM1555C1H100J
CN1	1	USB Micro B Connector	FCI	10103594-0001LF
D1	1	Orange LED (0603)	Panasonic	LNJ826W83RA
FB1, FB2	2	Ferrite (0603)	Murata Electronics North	BLM18KG221SN1D
J1	1	PMOD Receptacle	Samtec	SSW-106-02-T-S-RA
Q1	1	N-Channel MOSFET(SOT-23)	Diodes Inc.	2N7002-7
Q2	1	P-Channel MOSFET (SOT-23)	International Rectifier	PMV65XP,215
R1	1	10Ω Resistor (0603)	Vishay Dale	CRCW060310R0JNEA
R2	1	1.5kΩ Resistor (0402)	Vishay Dale	CRCW04021K50JNED
R3, R6, R7	3	100kΩ 1% Resistor (0402)	Vishay Dale	CRCW0402100KFKED
R4	1	32.4kΩ 1% Resistor (0402)	Vishay Dale	CRCW040232K4FKED
R5	1	4.7kΩ Resistor (0402)	Panasonic	ERJ-2GEJ472X
R8	1	1kΩ Resistor (0402)	Vishay Dale	CRCW04021K00JNED
R9	1	2.2kΩ Resistor (0402)	Panasonic	ERJ-2GEJ222X
R10	1	499Ω Resistor (0402)	Vishay Dale	CRCW0402499RFKED
R11	1	4.99Ω 1% 1/8W Resistor (0805)	Vishay Dale	CRCW08054R99FKEA
R12	1	680Ω Resistor (0402)	Panasonic	ERJ-2GEJ681X
R13, R14	2	1.74kΩ Resistor (0402)	Panasonic Electronic Co	ERJ-2RKF1741X
RT1	1	PTC Fuse (1206)	Bourns Inc.	MF-NSMF012-2
S1	1	Tactile Switch	Omron Electronics Inc	B3U-1000P
U1	1	Security Token Microcontroller with RTC and USB	Maxim Integrated	MAXQ1010-A01+
U2	1	High PSRR, Low-Dropout, 150mA Linear Regulator	Maxim Integrated	MAX8891EXK33+
U3	1	Dual High-Speed Differential ESD-Protection IC	Maxim Integrated	MAX3207EAUT+
U4	1	40ns Single-Supply Comparator	Maxim Integrated	MAX9140AAXK+
U5	1	4 Channel +/- 30kv ESD Protector	Maxim Integrated	MAX13204EALT+
X1	1	12MHz Crystal	EPSON	FA-238V 12.0000MB-K3
X2	1	Do Not Populate (3.20x1.50mm)		

DS9481P-300 Schematics



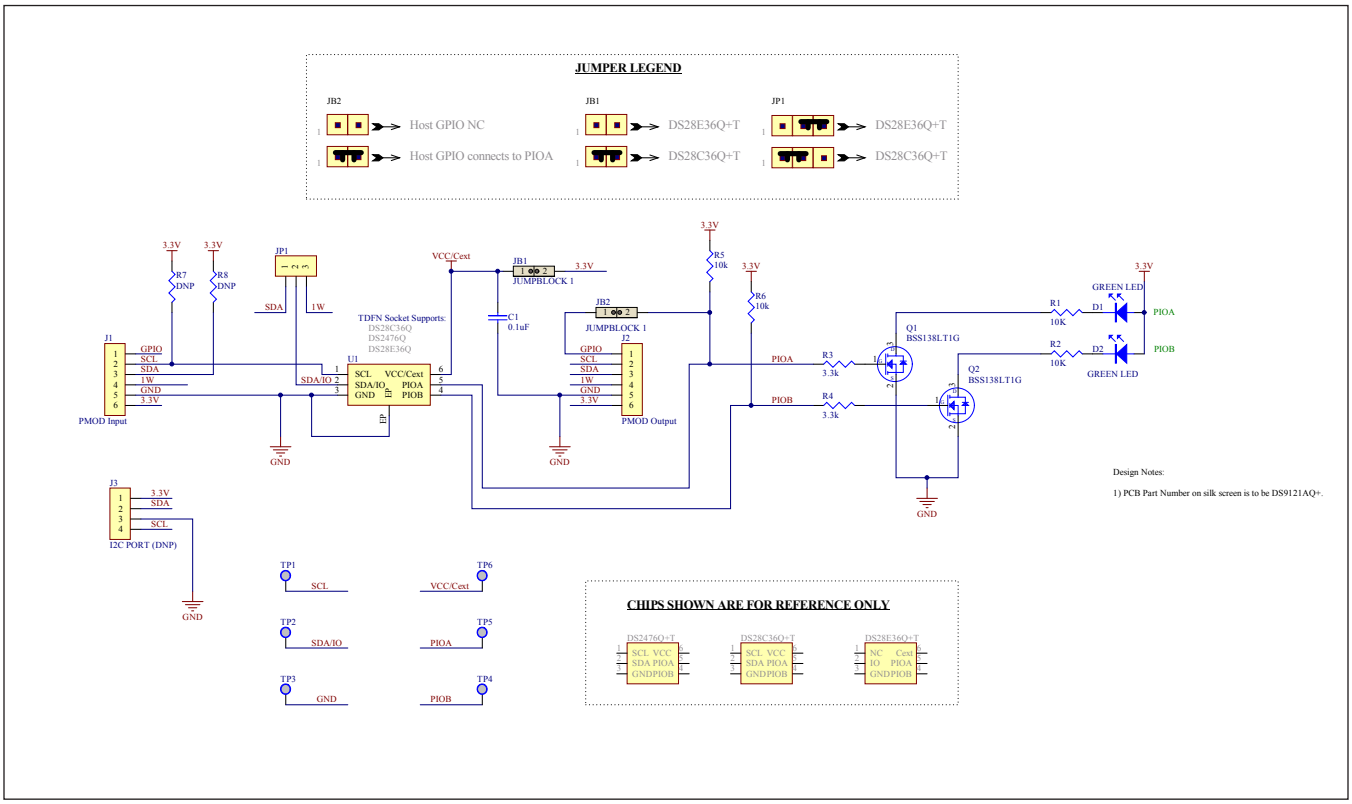
DS9481P-300 PCB Layout



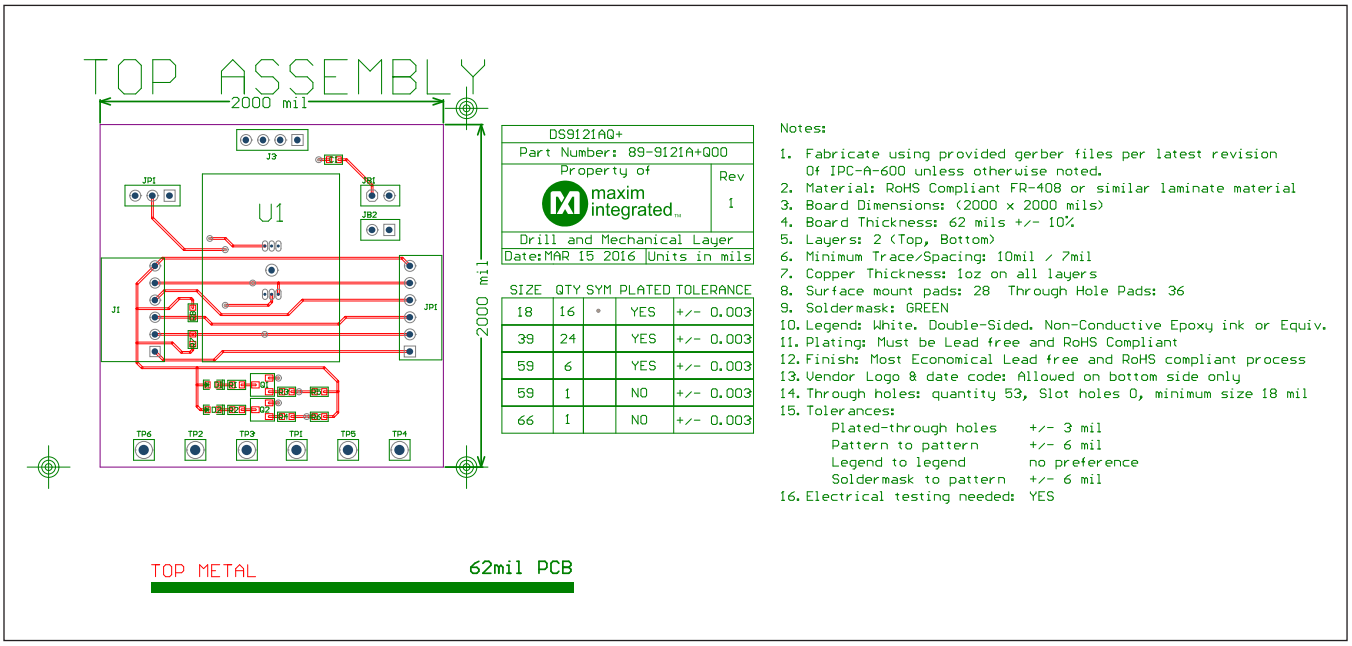
DS9121AQ Bill of Materials

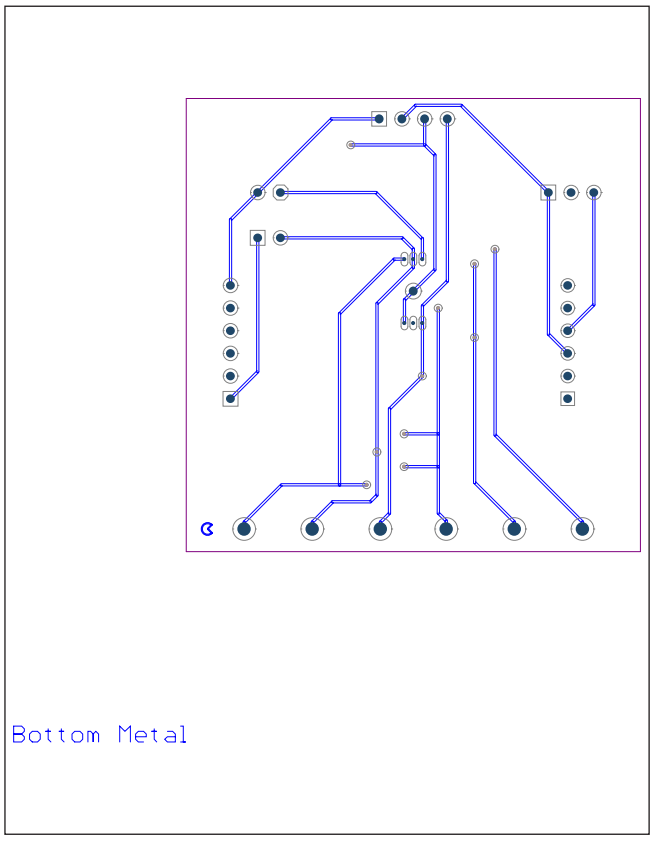
Designator	Quantity	Description	Manufacture Name	Part Number
J3	1	4 Pin 100mil Female Connector	Samtec	SSQ-104-02-T-S-RA
R3, R4	2	RES 3.3K OHM 1/10W 1% 0603 SMD	Panasonic Electronic Components	ERJ-3EKF3301V
R1, R2, R5, R6	4	RES SMD 1K OHM 1% 1/10W 0603, RES SMD 10K OHM	Panasonic Electronic Components	ERJ-3EKF1002V
R7, R8	2	RES SMD 10K OHM 1% 1/10W 0603	Panasonic Electronic Components	ERJ-3EKF1002V
C1	1		Kemet	C0603C104K8RACTU
Q1, Q2	2	MOSFET N-CH 50V 200MA SOT-23	ON SEMICONDUCTOR	BSS138LT1G
D1, D2	2	LED INGAN GREEN CLEAR 0603 SMD	Dialight	598-8081-107F
J1	1	CONN HEADER FEMALE 6POS .1" GOLD	TE Connectivity	9-146285-0
J2	1	CONN HEADER FEMALE 6POS .1" GOLD	TE Connectivity	9-146285-0
JP1	1	HDR,BRKWAY,.100 3POS VERT,0.318"	Tyco Electronics	9-146276-0
U1	1	TDFN,3MM,x2,CLAMSHELL,BURNIN	PLASTRONICS	06QN10T23030
JB1, JB2	2	JUMPER BLOCK, .100 2POS VERT,0.318"	Tyco Electronics	22-28-4363
Pack Out	3	SHUNT+,LP W/HANDLE 2 POS 30AU	Tyco Electronics	881545-2

DS9121AQ Schematics



DS9121AQ PCB Layout





Revision History

REVISION NUMBER	REVISION DATE	DESCRIPTION	PAGES CHANGED
0	8/16	Initial release	—
1	5/17	Added DS29E36 to data sheet, updated Figures 10, 13-15, 25, 27-29	1–30

