

DS28E38 Evaluation System

Evaluates: DS28E38 and DS2476

General Description

The DS28E38 evaluation system (EV system) provides the hardware and software necessary to exercise the features of the DS28E38 and DS2476. The EV system consists of five DS28E38/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 under Windows[®] 10, Windows 8, and Windows 7 operating systems, both 64-bit and 32-bit versions. It provides a handy user interface to exercise the features of the DS28E38 and DS2476.

EV Kit Contents

QTY	DESCRIPTION
5	DS28E38Q+ DeepCover Secure Authenticator with ChipDNA PUF Protection (6 TDFN)
5	DS2476Q+ DeepCover Secure Coprocessor (6 TDFN)
2	DS9121AQ+ Socket Board (6 TDFN)
1	DS9481P-300# USB to 1W/I ² C Adapter
1	USB Type-A to Micro-USB Type-B Cable

Features

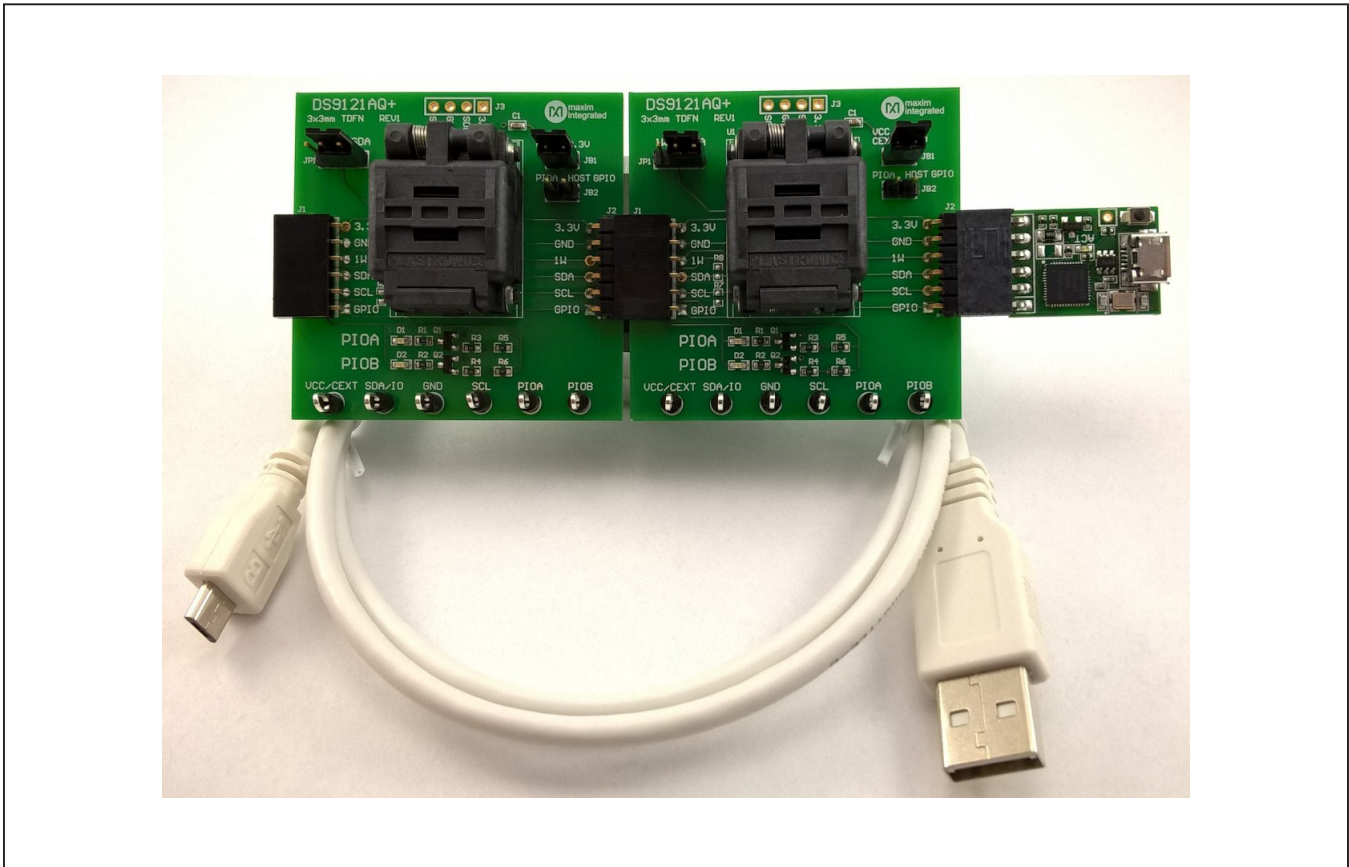
- Demonstrates the Features of the DS28E38 DeepCover[®] Secure Authenticator with ChipDNA PUF Protection
- Demonstrates the Features of the DS2476 DeepCover Secure Coprocessor
- 1-Wire/I²C Communication Is Logged to Aid Firmware Designers Understanding of DS28E38 and DS2476
- 1-Wire/I²C USB Adapter Creates 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, TDFN Socket
- Evaluation Software Available by Request

Ordering Information appears at end of data sheet.

1-Wire and DeepCover are registered trademarks of Maxim Integrated Products, Inc.

Windows is a registered trademark and registered service mark of Microsoft Corporation.

DS28E38 EV System



Quick Start

This section includes a list of recommended equipment and instructions on how to set up the Windows-based PC for the evaluation software.

Required Equipment

- DS9481P-300# USB to 1-Wire/I2C adapter (included)
- DS9121AQ+ TDFN socket board (two included)
- DS28E38Q+ (five devices included)
- DS2476Q+ (five devices included)

- USB Type A to Micro-USB Type B cable (included)
- PC with a Windows 10, Windows 8, or Windows 7 operating system (64 bit or 32 bit) and a spare USB 2.0 or higher port
- Download DS28E38 EV kit software (light version) or request [full DS28E38 EV kit developer software](#).

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

Hardware Setup and Driver Installation Quick Start

The following steps were performed on a Windows 7 PC to set up the DS28E38 EV kit hardware/software:

1) Obtain and unpack the **DS28E38_EV_Kit_Software**

Setup_V1.0.0.zip file, or the latest version.

2) In a file viewer ([Figure 1](#)), double click on **DS28E38_EV_Kit_Software_Setup_V1.0.0.exe** to begin the installation.

3) The setup wizard opens; click on **Next**, as shown in [Figure 2](#).

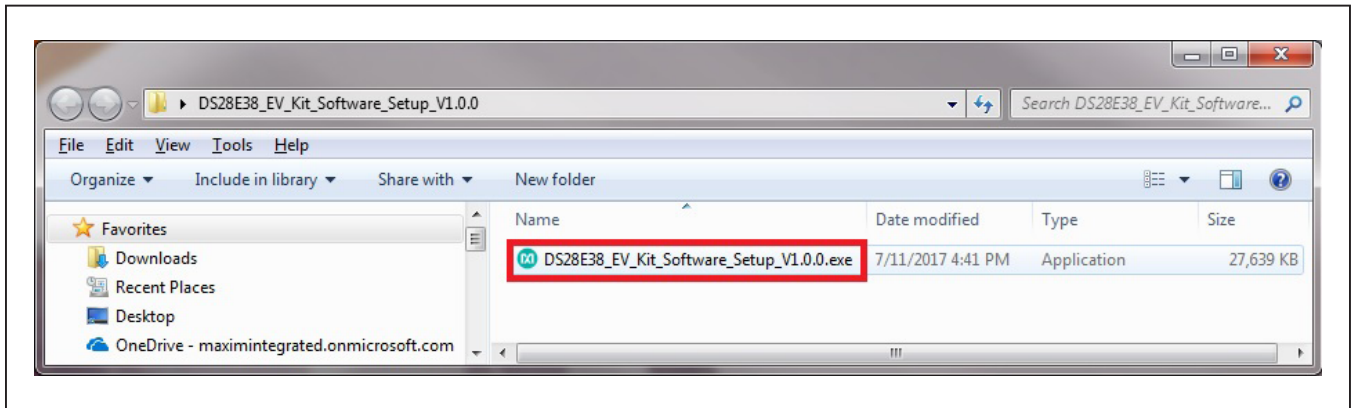


Figure 1. File Viewer

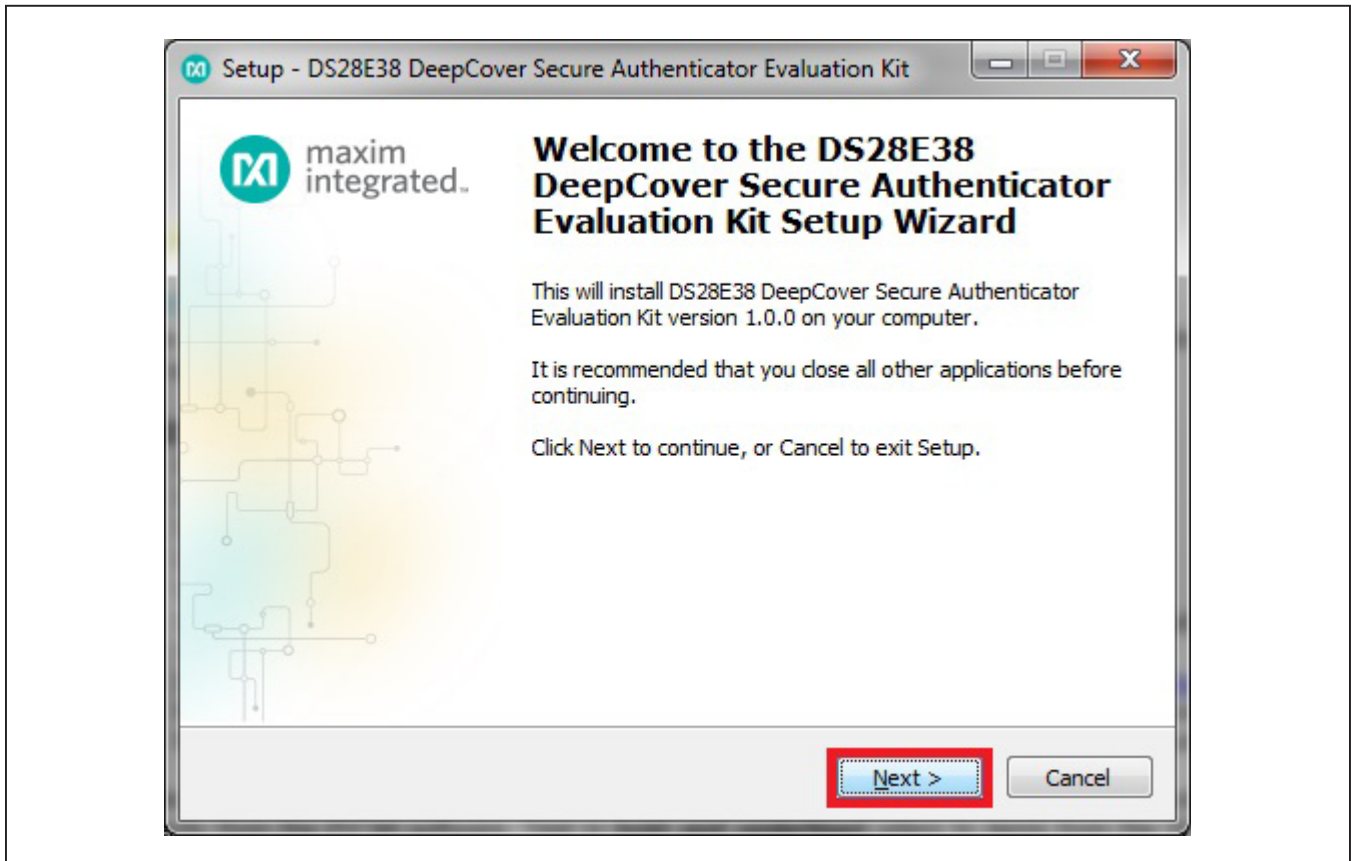


Figure 2. DS28E38 Setup Wizard

- 4) Click **Browse** to select a default folder location, and then click **Next** to install the EV kit software (Figure 3).

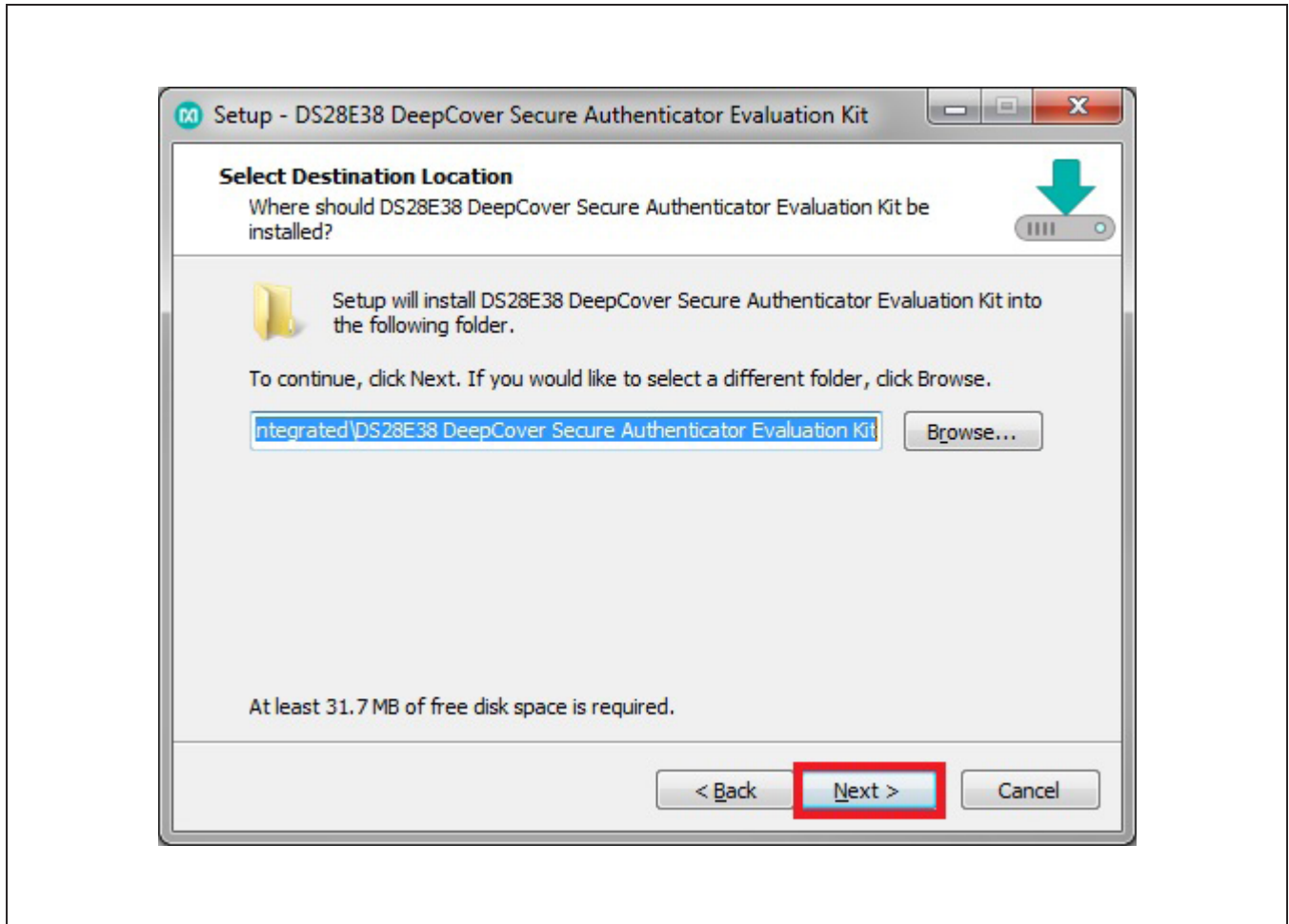


Figure 3. Install Folder Location

5) Click **Next** to install shortcuts to the default folder (Figure 4).

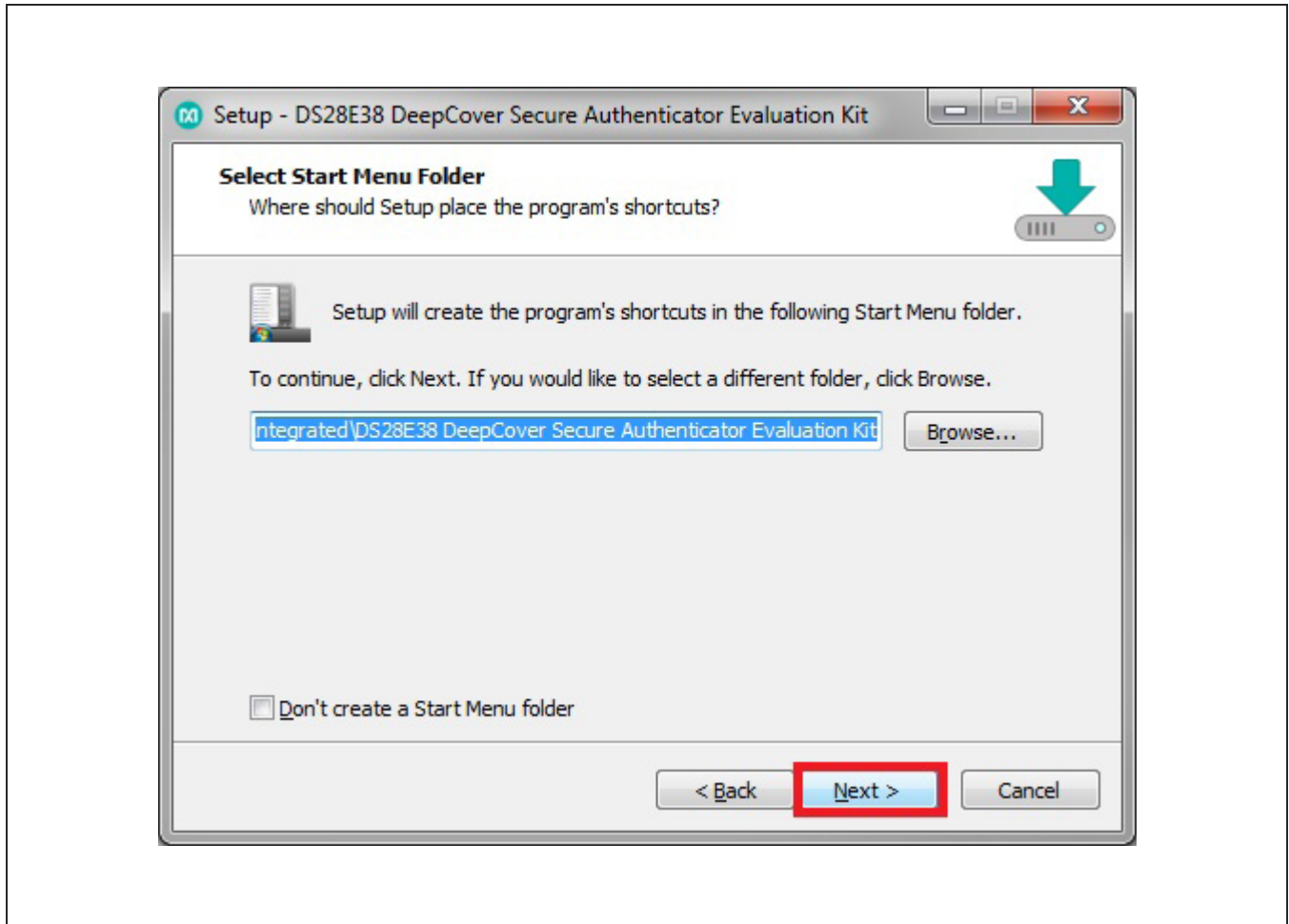


Figure 4. Program Shortcuts Location

- 6) Unplug any Maxim adapter and click on **Next**, with the default settings checked. This selects and installs the DS9481P-300# driver, which is needed to communicate through the USB via a virtual COM port (Figure 5).

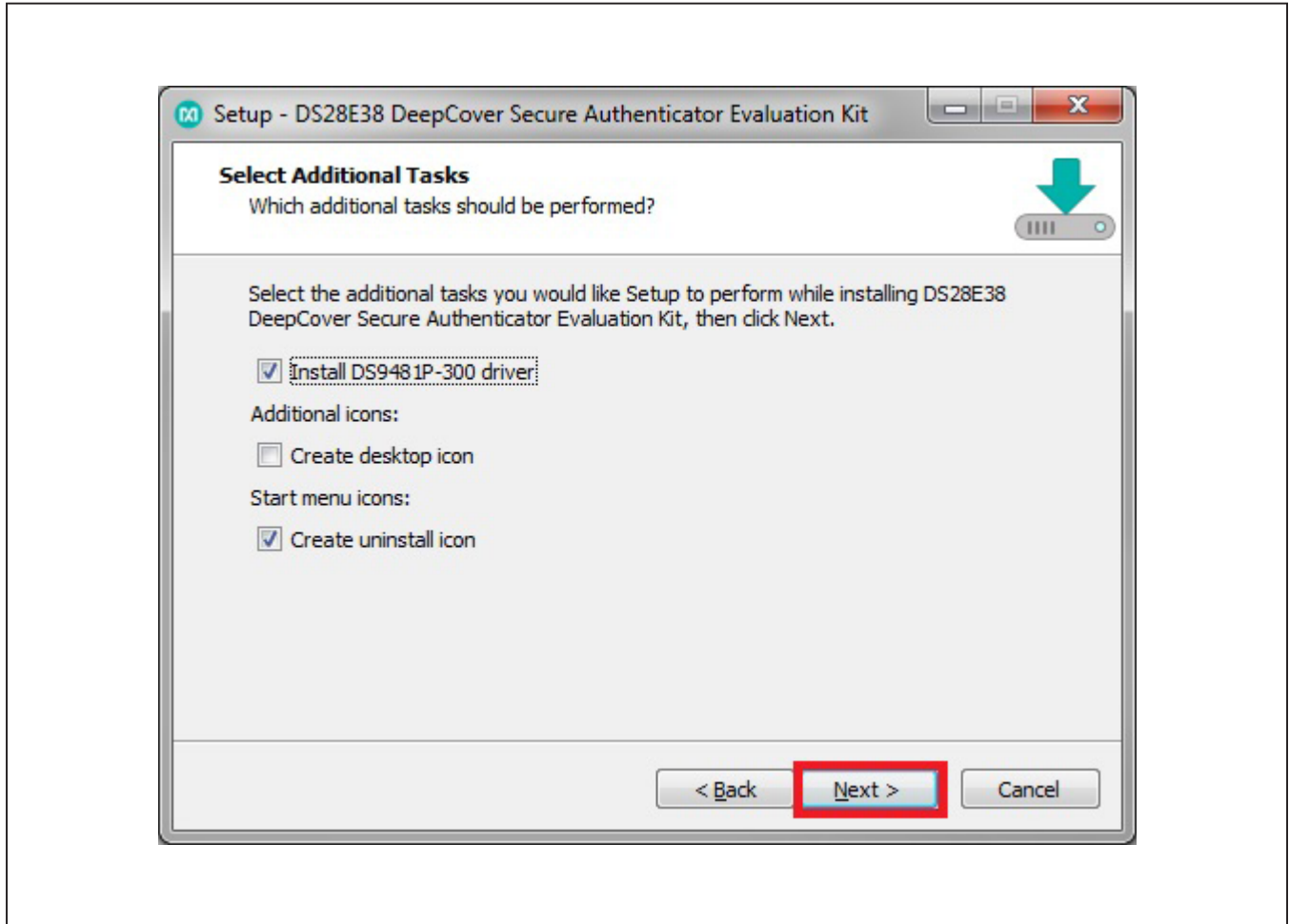


Figure 5. Select to Install the Driver

7) Next click on **Install**. A new window pops up to show the installing progression (Figure 6).

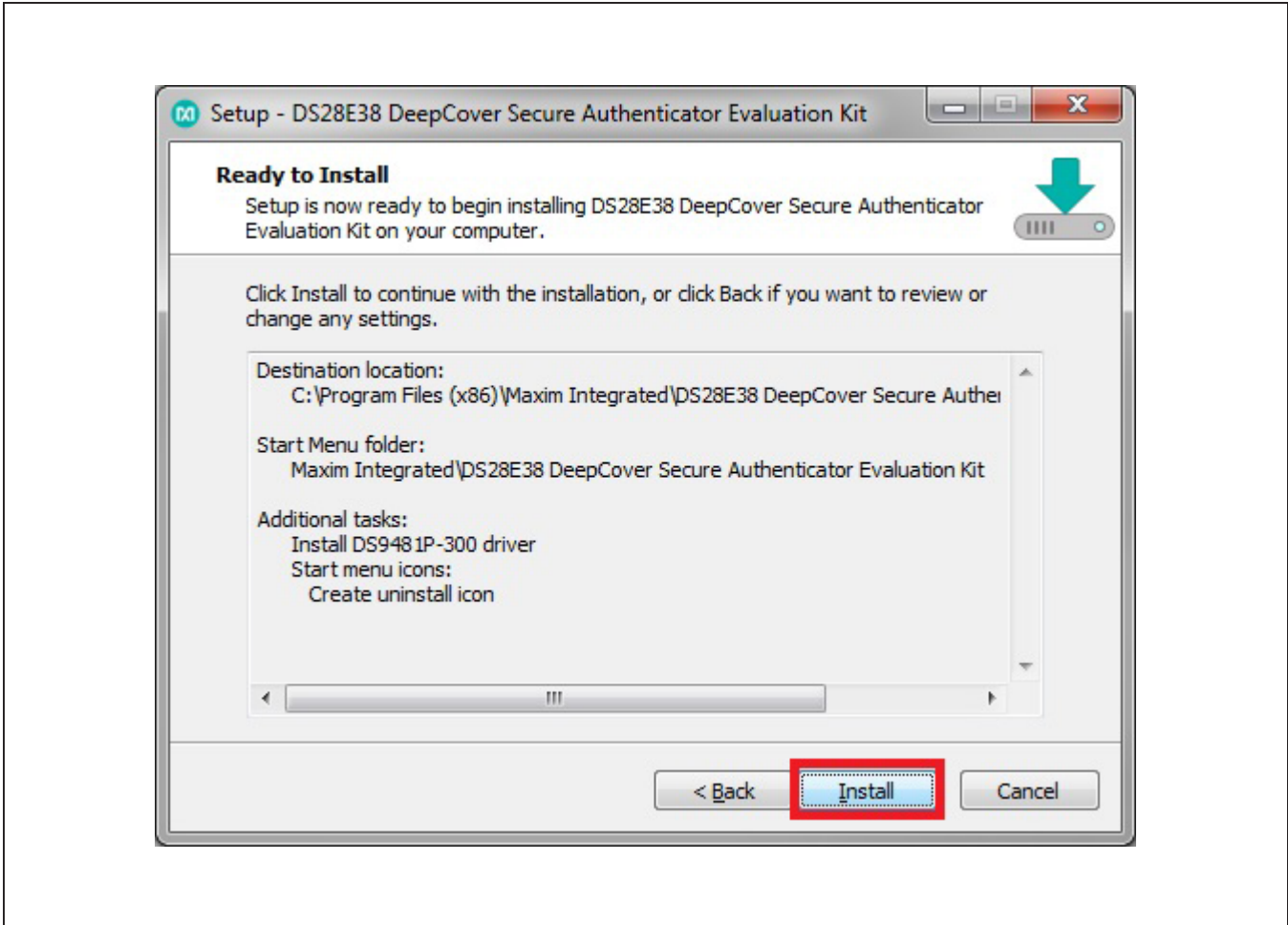


Figure 6. Ready to Instal

8) Click on **Next** when the Device Driver Installation Wizard appears (Figure 7).

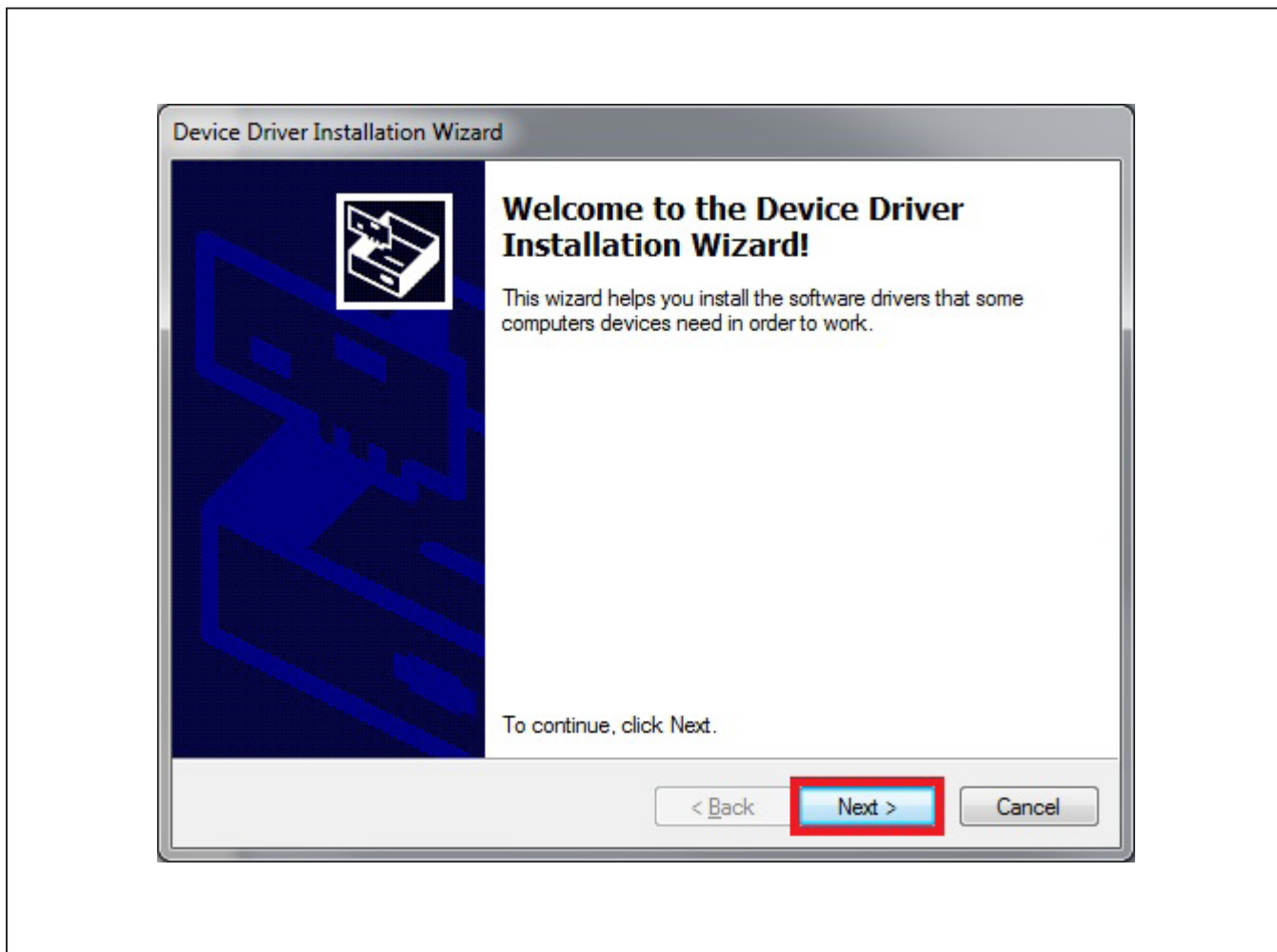


Figure 7. Device Driver

9) Click on **Finish** to close the final window and confirm the driver is installed correctly (Figure 8).

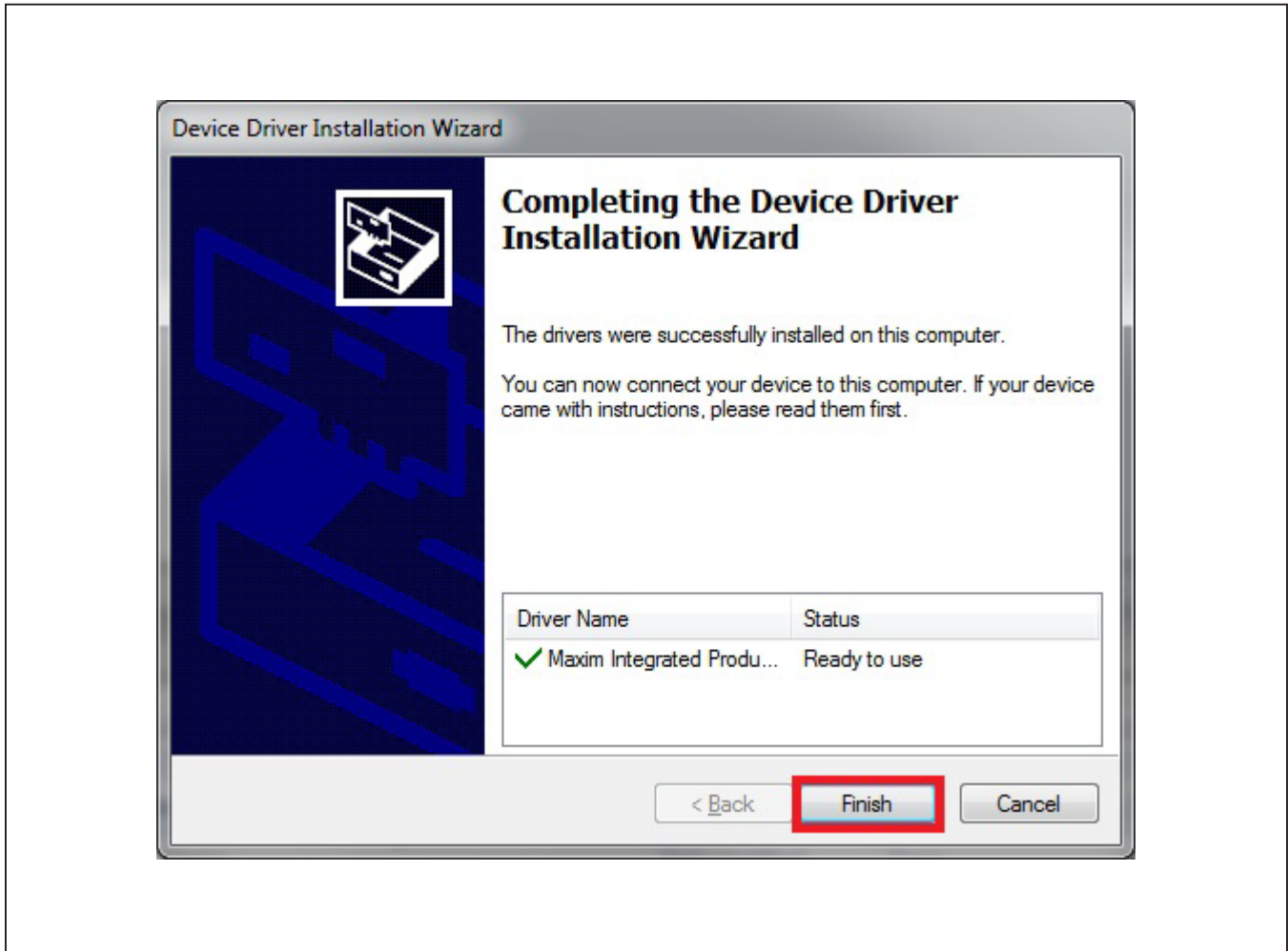


Figure 8. Device Driver Installation Finished

DS28E38 Evaluation System

Evaluates: DS28E38 and DS2476

- 10) Plug the DS9481P-300# into the PC with both DS9121AQ+ socket boards by doing the following:
 - a) (Optional—Perform only if using the coprocessor): Open the 1st socket and insert a DS2476 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 2nd socket and insert a DS28E38 into one of the cavities, per the same orientation shown in [Figure 9](#).
 - c) Close both burn-in sockets.
 - d) Connect the 1st DS9121AQ J2, 6-pin female socket, into the DS9481P-300#, 6-pin male plug per [Figure 10](#).
 - e) Connect the 2nd DS9121AQ J2, 6-pin female socket, into the 1st DS9121AQ J1, 6-pin male plug per [Figure 10](#).
 - f) For the 1st DS9121AQ+ socket boards that contains DS2476, configure jumpers JP1 to use SDA and JB1 to use 3.3V per [Figure 10](#).
 - g) For the 2nd DS9121AQ+ socket boards that contains DS28E38, configure jumpers JP1 to use 1W and JB1 do not install per [Figure 10](#).
 - h) Plug the DS28C36 EV kit, using a USB Type-A to Micro-USB Type-B cable, into the PC.

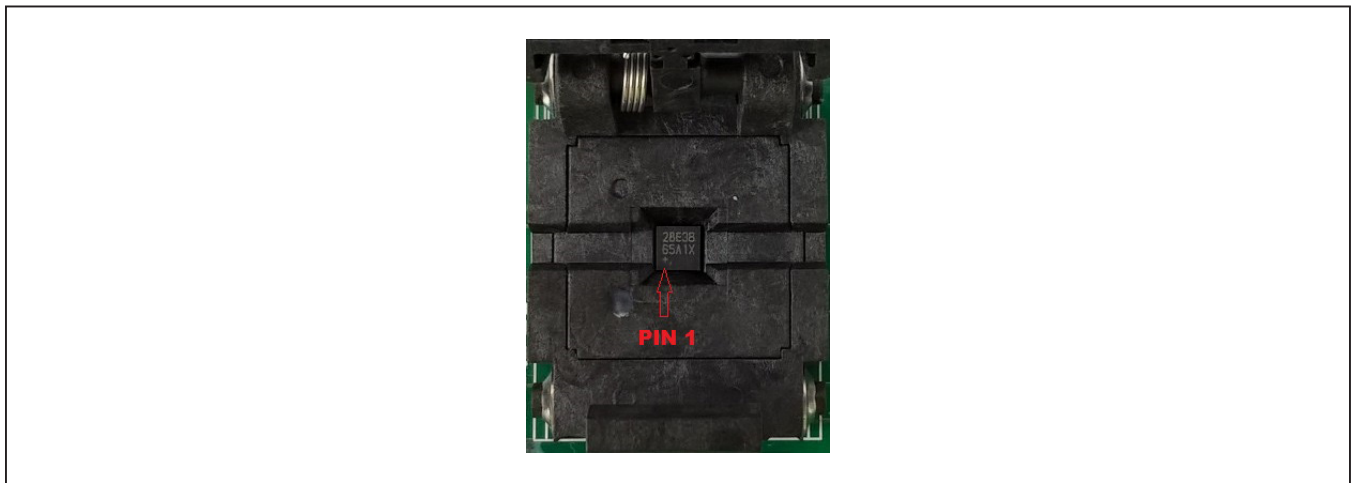


Figure 9. Orientation of the DS28E38 and DS2476 in the Burn-In Socket

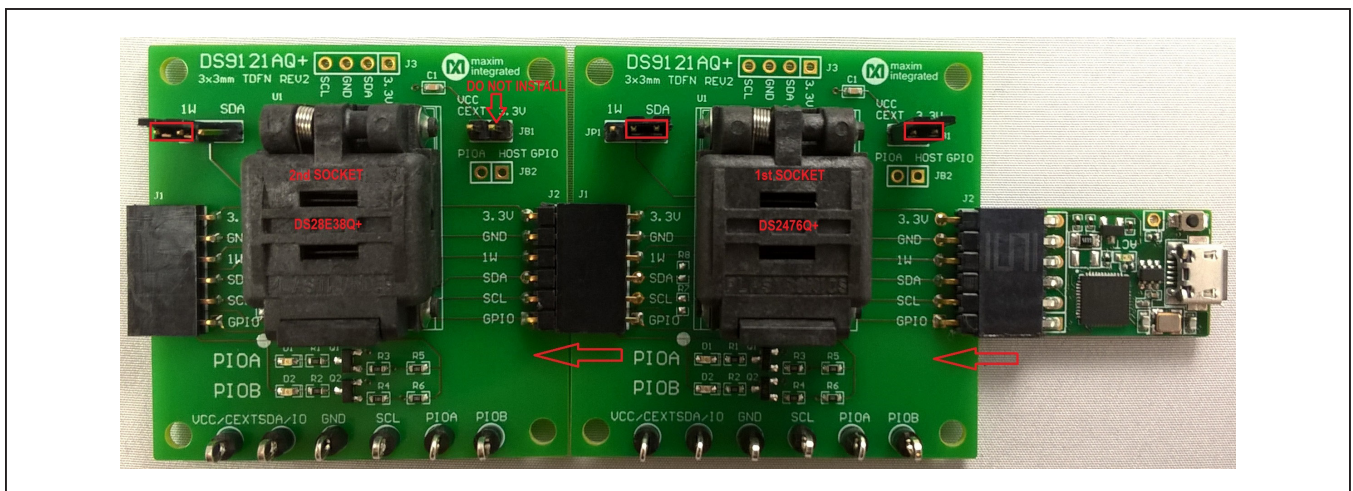


Figure 10. DS9481QA-300# and DS9121AQ

11) Click on **Finish** to close the final window and confirm the software is installed correctly (Figure 11).

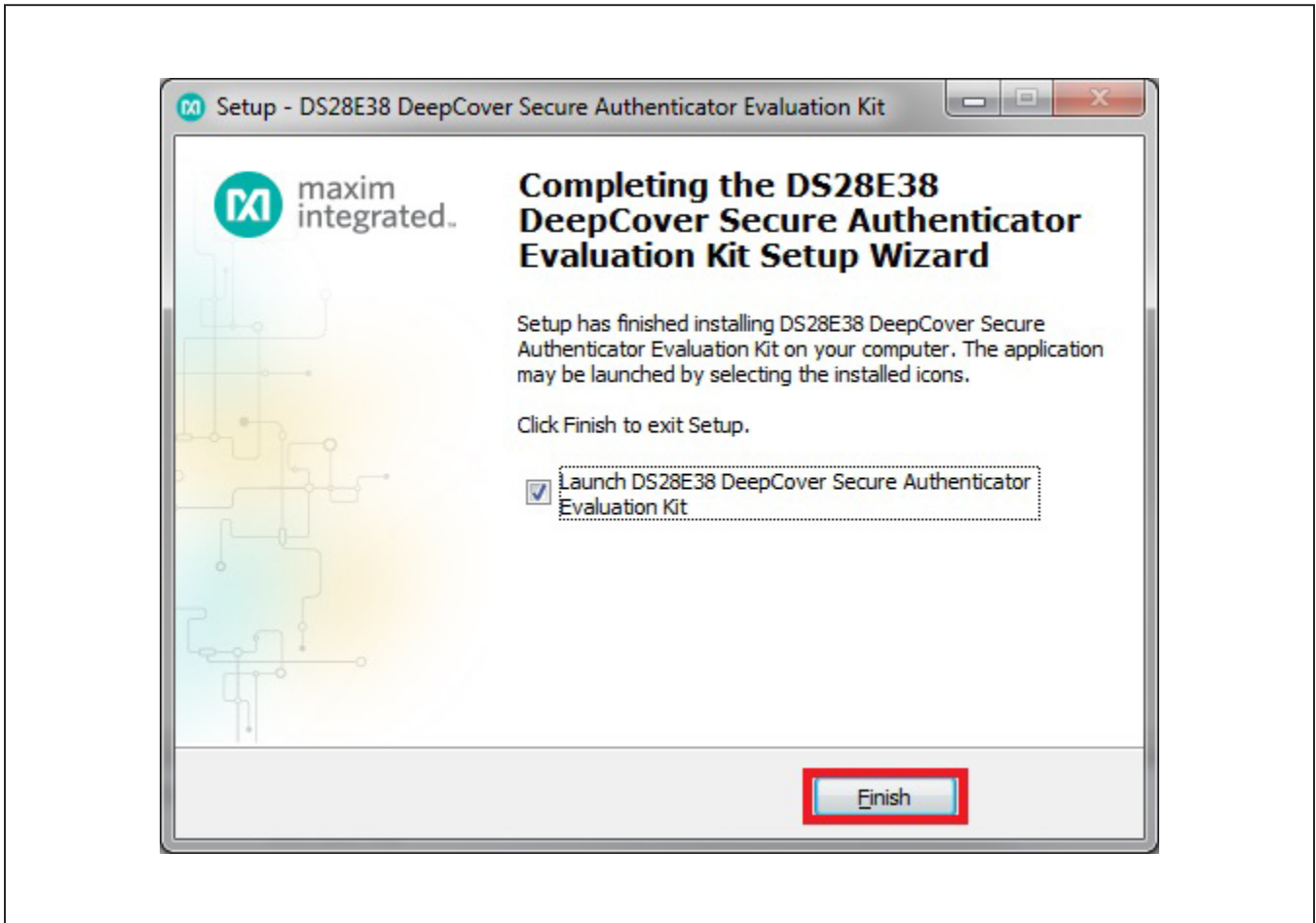


Figure 11. Software Installation Finished

12) The DS28E38 EV kit program opens and automatically connects to the COM port. This can be verified

in the lower right corner of the window, as shown in [Figure 12](#).

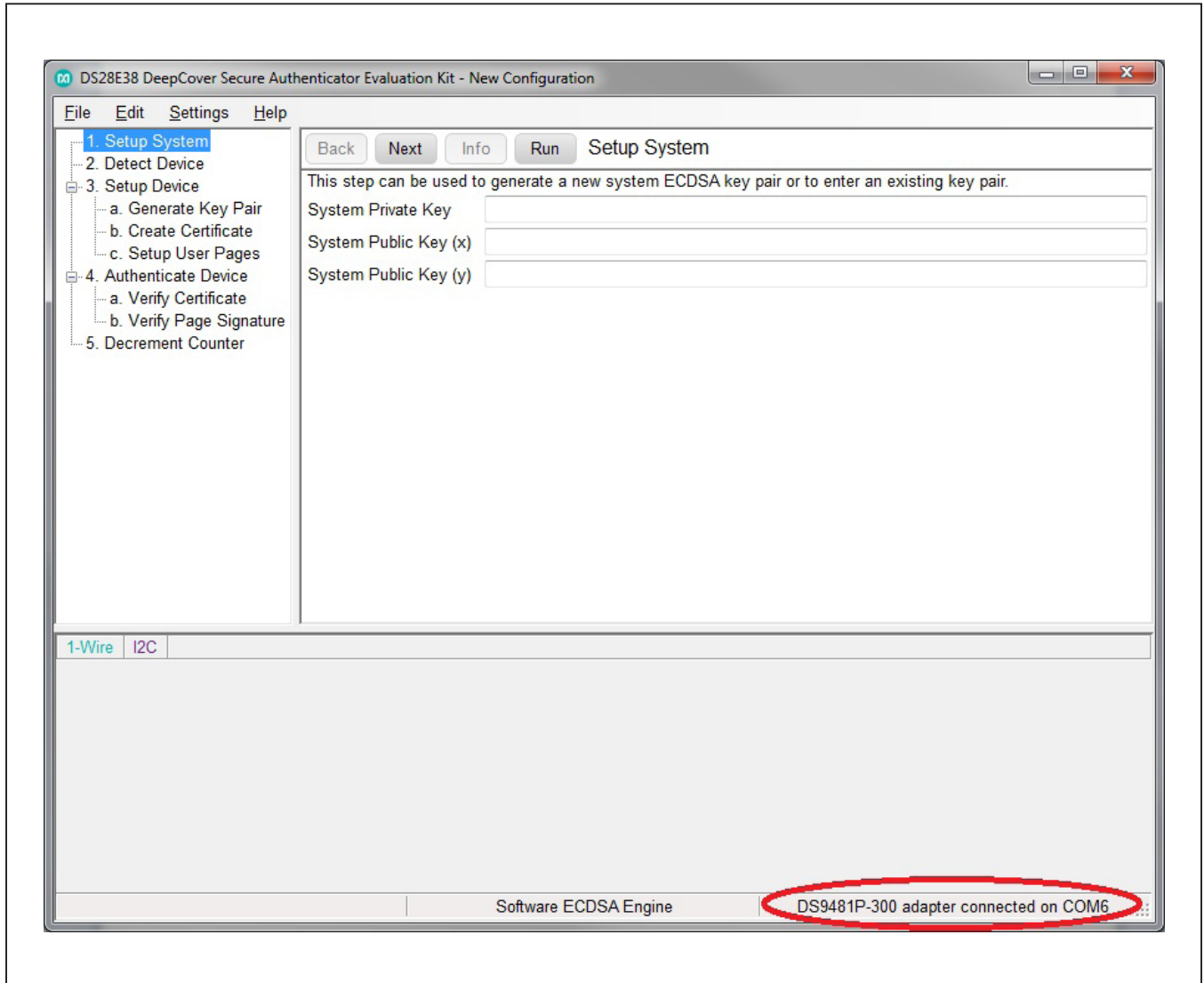


Figure 12. DS28E38 EV Kit Program (Default View Upon Opening)

Usage Example—Feature (User Memory) Authentication with ECDSA

The DS28E38 EV kit program is designed as a usage example to show, step by step, how to set up and then authenticate a user memory page of the DS28E38 slave device. It includes the ability to either use the software ECDSA engine built in, or a DS2476Q+ coprocessor for the host compute engine. The default is to use the software ECDSA engine. To use the coprocessor, go under the toolbar **Settings** and then **ECDSA Engine**, and select **DS2476**. The GUI displays all the I²C and 1-Wire sequences for each step performed to assist the firmware engineer.

Setup

This section includes steps to set up the host and DS28E38. This is typically done during manufacturing at a secure location. See steps 1 through 3.

Step 1: Setup System

The system ECDSA key pair needs to be generated prior to any other steps. The system private key should always be kept hidden and in a secure location. With the **Setup System** selected (i.e., highlighted dark gray), click the **Run** button to automatically generate the system ECDSA key pair and then click on **Next** to move to the next step ([Figure 13](#)).

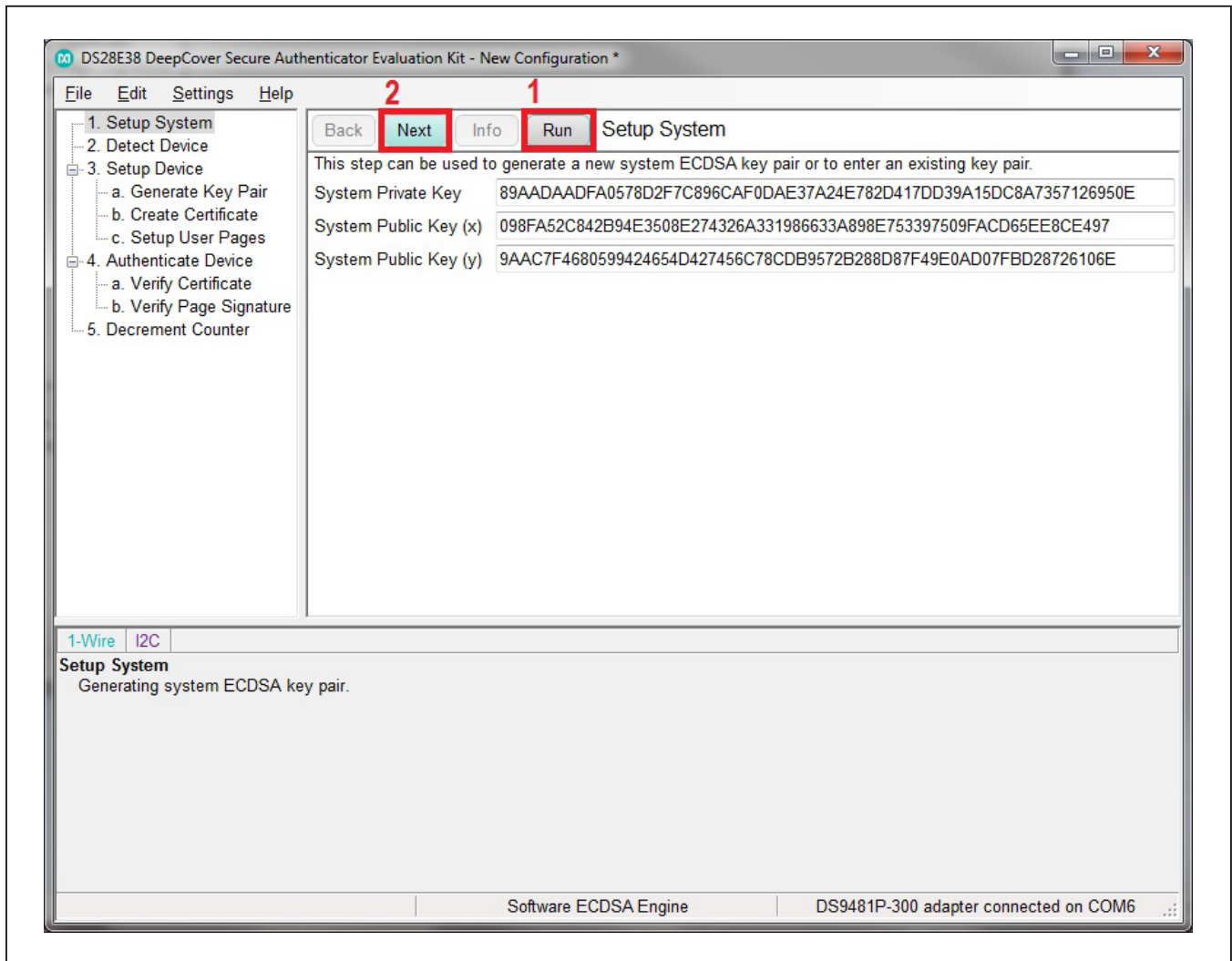


Figure 13. Generating System ECDSA Key Pair

Step 2: Detect Device

Each DS28E38 device contains a unique 64-bit ROM ID and 16-bit MAN ID that are ingredients used during the generate key pair, and create certificate steps. Click on the **Run** button to read the status info of the ROM ID and MAN ID. Then click on **Next** twice to move to subitem step 3a (Figure 14).

Step 3: Device Setup

Each DS28E38 device needs to have its own unique device key pair internally, and a stored certificate generated by the system private key. The user should set up the

desired data for the user pages and, if desired, set up the decrement counter when needed.

- a. To set up the device, first generate and store the device key pair by sending the proper commands to the DS28E38 device. Notice the parameter **Read Protection** is always selected since the private key is never readable. However, it is optional to select **Lock Key Pages**. Locking the key pages is recommended to minimize a competitor hacker from disrupting the device key pair and causing the device to not authenticate; however, for this example, the **Lock Key Pages** can be left unchecked. Generate the device

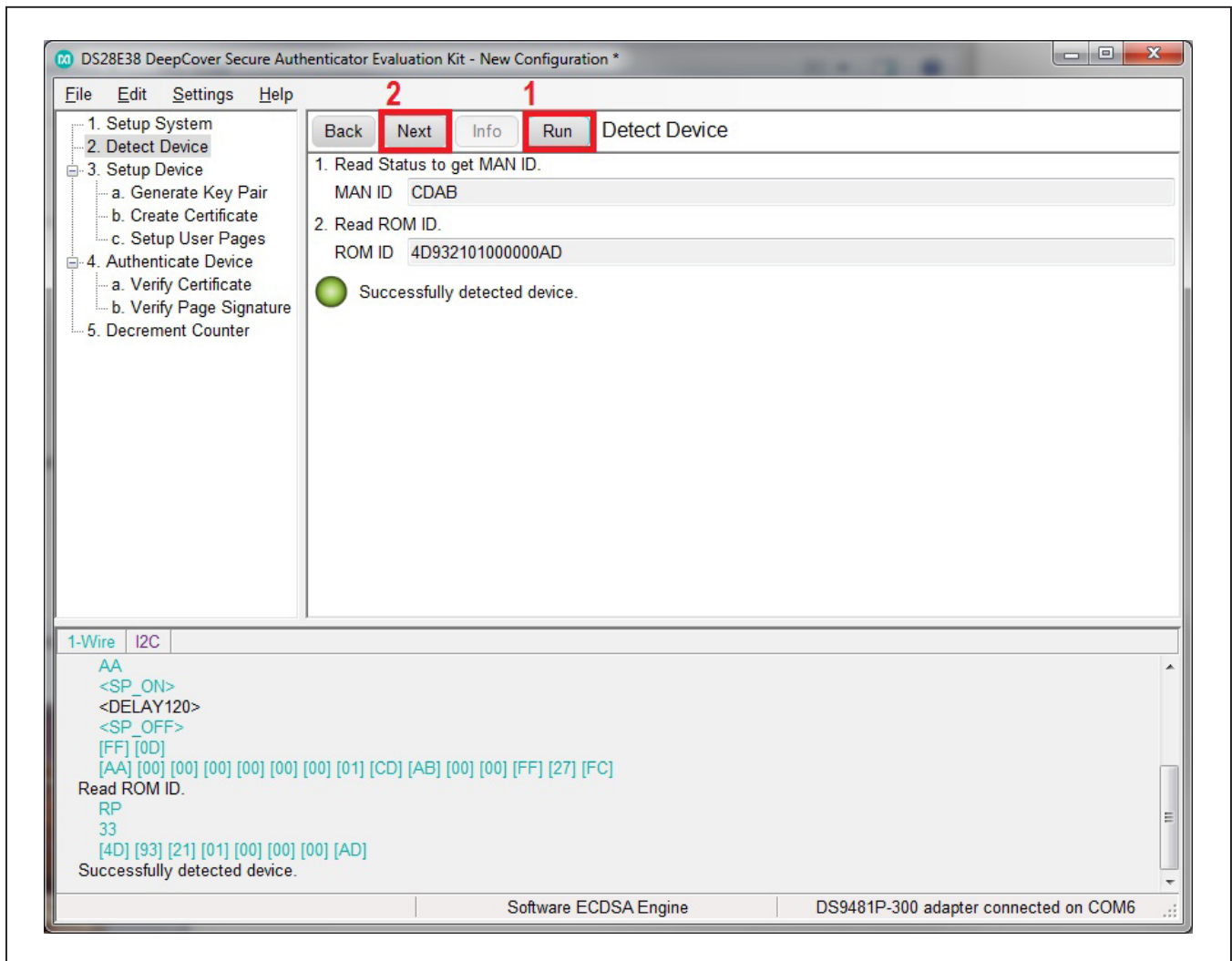


Figure 14. Detect Device

key pair by clicking on the **Run** button and observe the **Device Public Key** x/y generated can be seen, but not the **Private Key**. Now, click the **Next** button to move to step 3b (Figure 15).

b. The host can now generate the certificate with all the ingredients now available (i.e., system private key, device public key, ROM ID, MAN ID, and RNG). Click the **Run** button and observe the **Certificate**

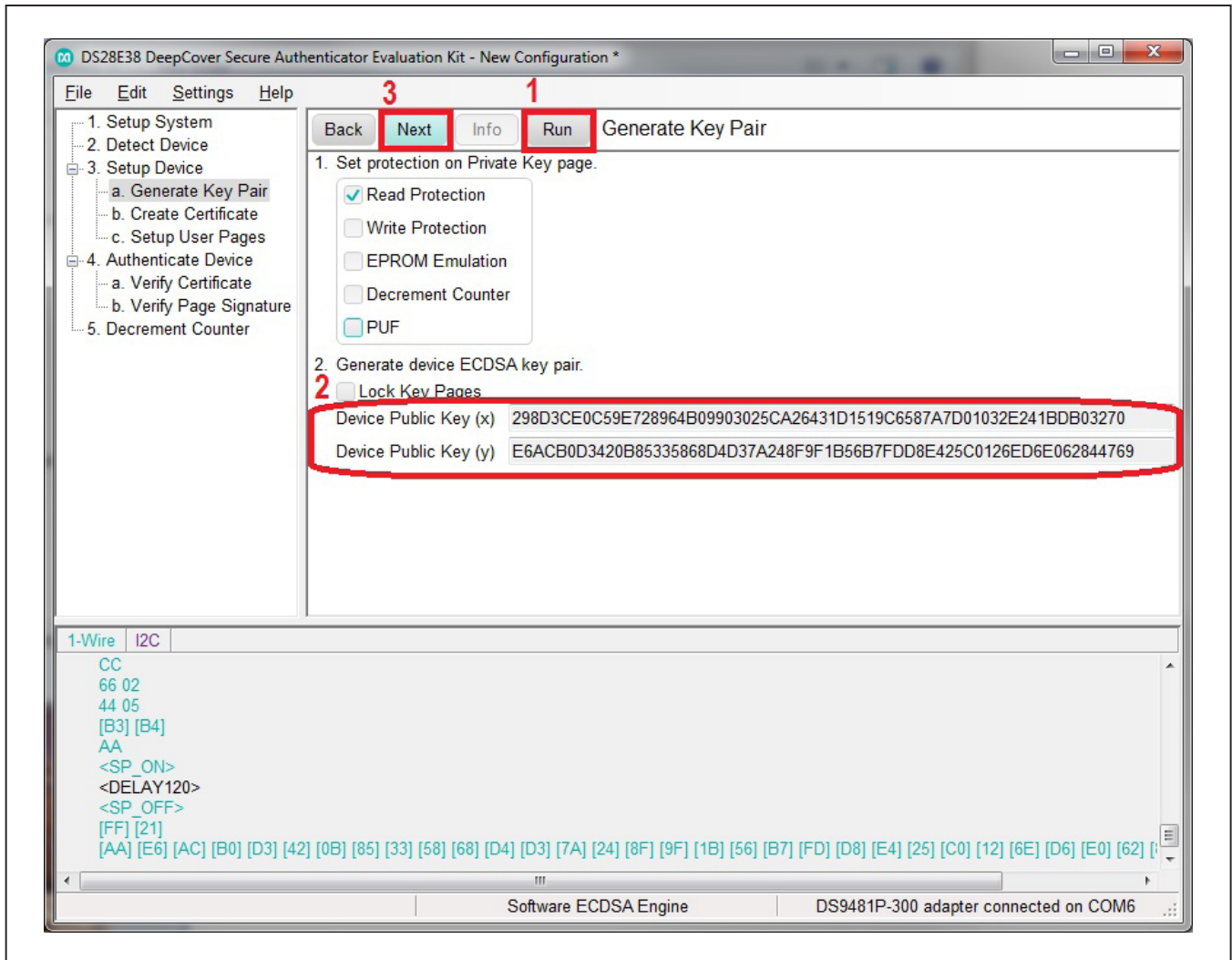


Figure 15. Device Key Pair Generation

created (Figure 16). Additionally, the run also writes the R-component of the certificate to page 0 and the S-component of the certificate to page 1. Click on the **Info** button and a window pops up that shows all the ingredients used to create the certificate (Figure 17). Close the **Create Certificate** ingredients window and click the **Next** button to step 3c.

c. In the **Page Data** field of **Page 2**, the desired user data can be entered. Enter the string-**000102030405060708090A0B0C0D0E0F101112131415161718191A1B1D1E1F20** that also corresponds to the byte order from byte 0 to byte 31. In the **Page Data** field of **Page 3**, it can be set up to be used for user data or for the decrement counter. In this case, the 17-bit decrement counter is used. The first three

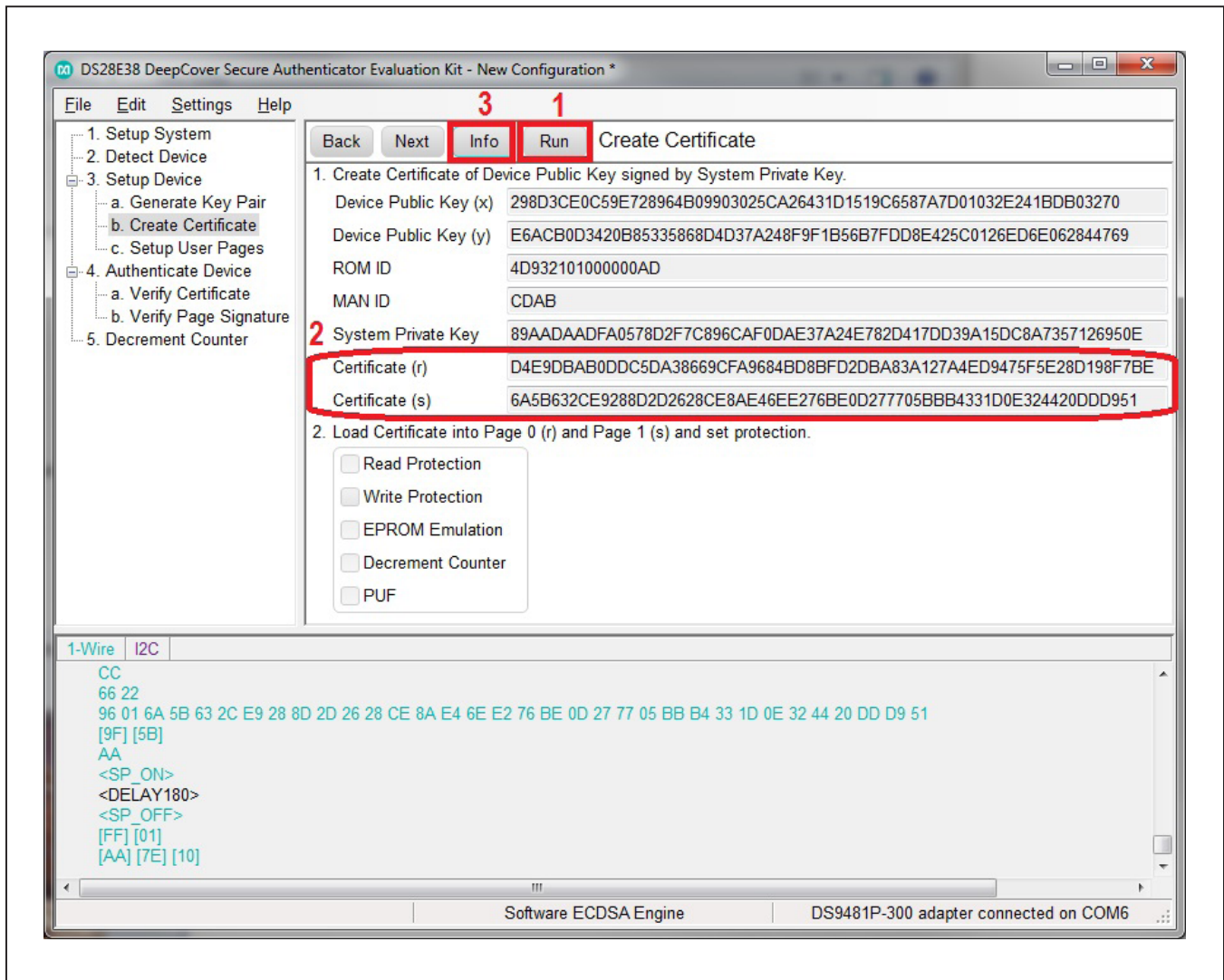


Figure 16. Create Certificate

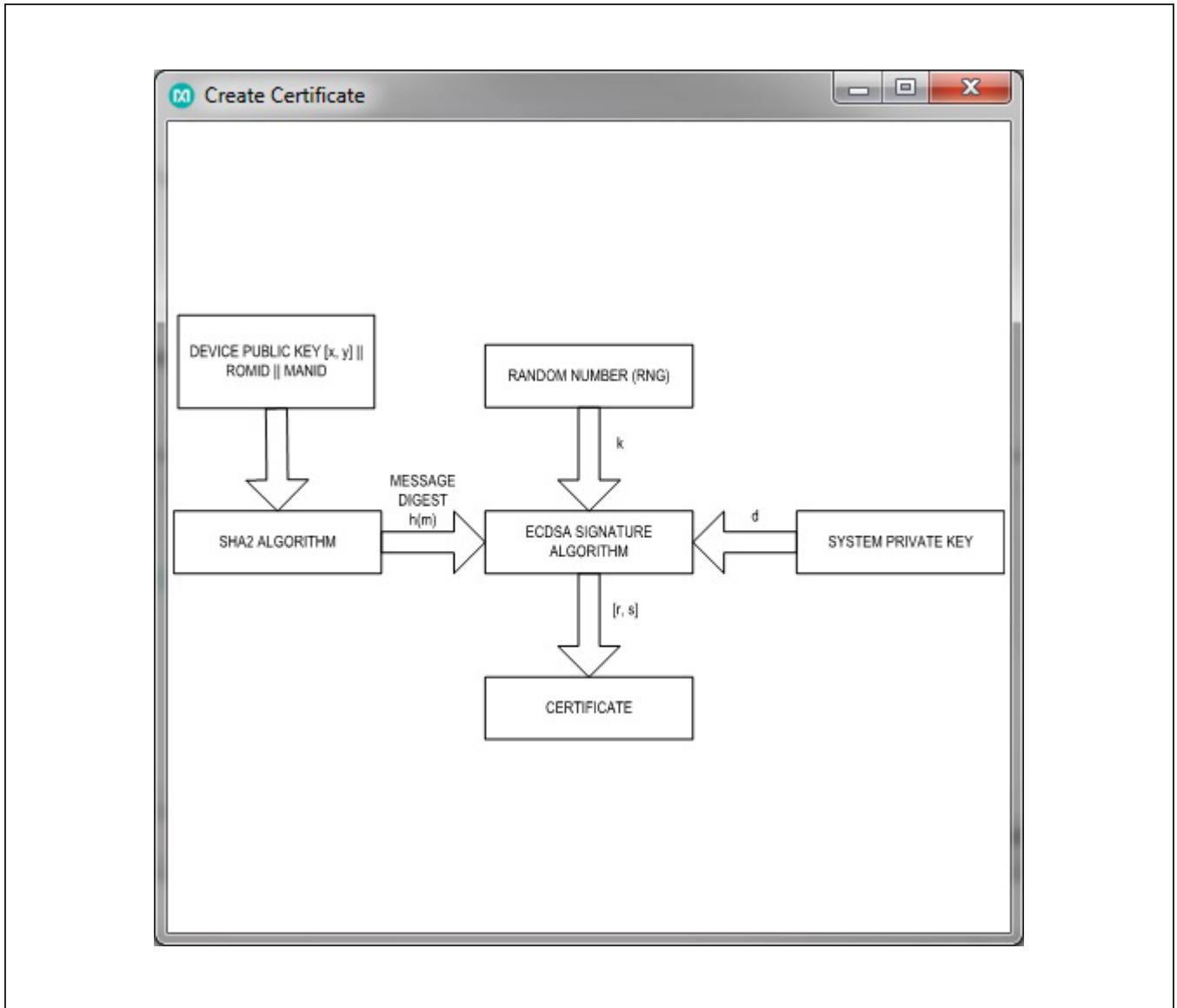
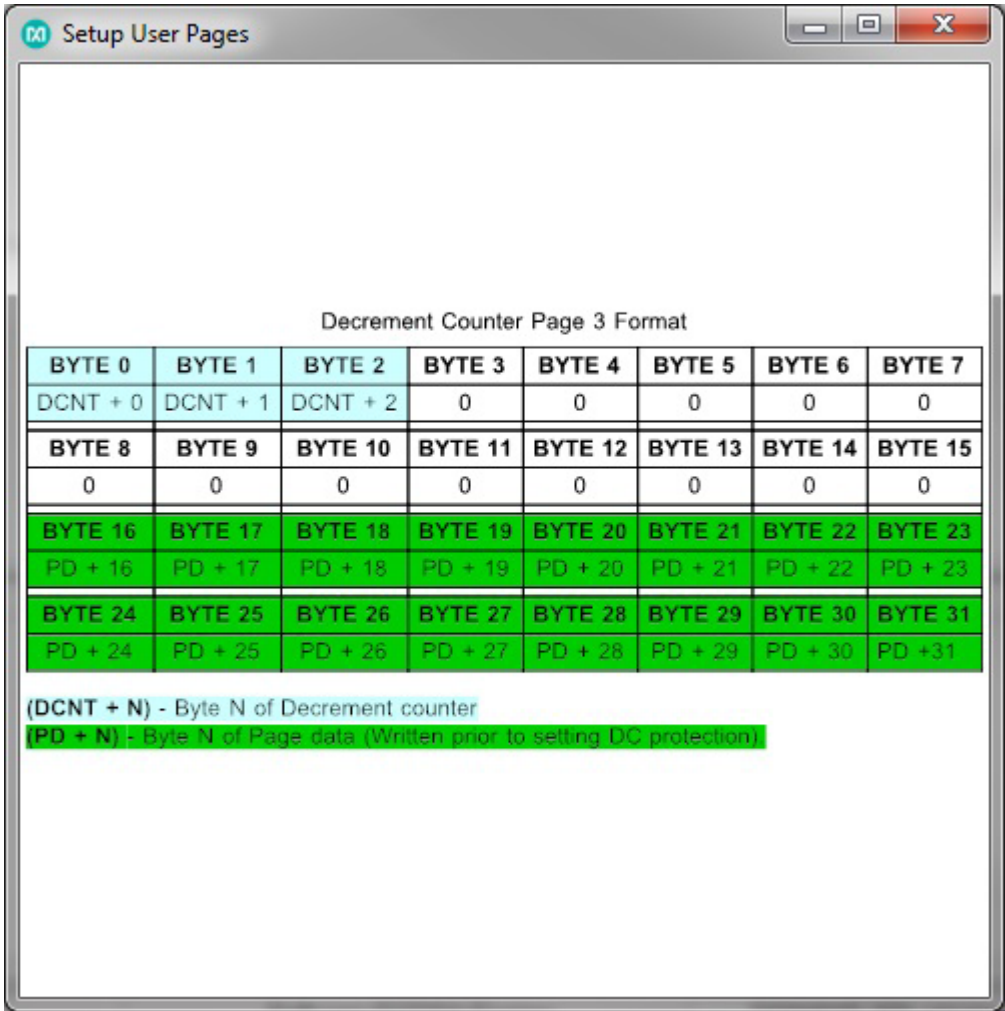


Figure 17. Ingredients Needed to Create the Certificate



The screenshot shows a window titled "Setup User Pages" with a table titled "Decrement Counter Page 3 Format". The table is divided into three sections: bytes 0-7, bytes 8-15, and bytes 16-31. The first two sections have values of 0, while the last section lists page data (PD) addresses. Below the table, there are two legend entries: "(DCNT + N) - Byte N of Decrement counter" and "(PD + N) - Byte N of Page data (Written prior to setting DC protection)".

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)

Figure 19. Decrement Counter Page 3 Format

Usage (Read Feature)

This section details the steps to authenticate DS28E38Q to the host.

Step 4: Authenticate Device

This step contains the operations to authenticate the DS28E38Q to the host. The step is broken up to two subitems to better describe the process. Click on **Next** to proceed to the first subitem.

- a. The host needs to check that the DS28E38 is part of the system by verifying its certificate. Click on **Run** button and confirm the status says, **Successfully verified Certificate** (Figure 20). During the run, the

host first read the certificate pages and populated the certificate r/s fields. Then the host read the device public keys x/y pages and populated the device public keys x/y fields. By the host gathering all these ingredients, it then could verify the certificate with the device public key, ROM ID, MAN ID and system public key which could have only been confirmed by the one certificate previously generated in the step 3b. Now click on the **Info** button and a window will pop up that shows all the ingredients used in the verification of the certificate (Figure 21). Close the **Verify Certificate** ingredients window and click the **Next** button to proceed to step 4b.

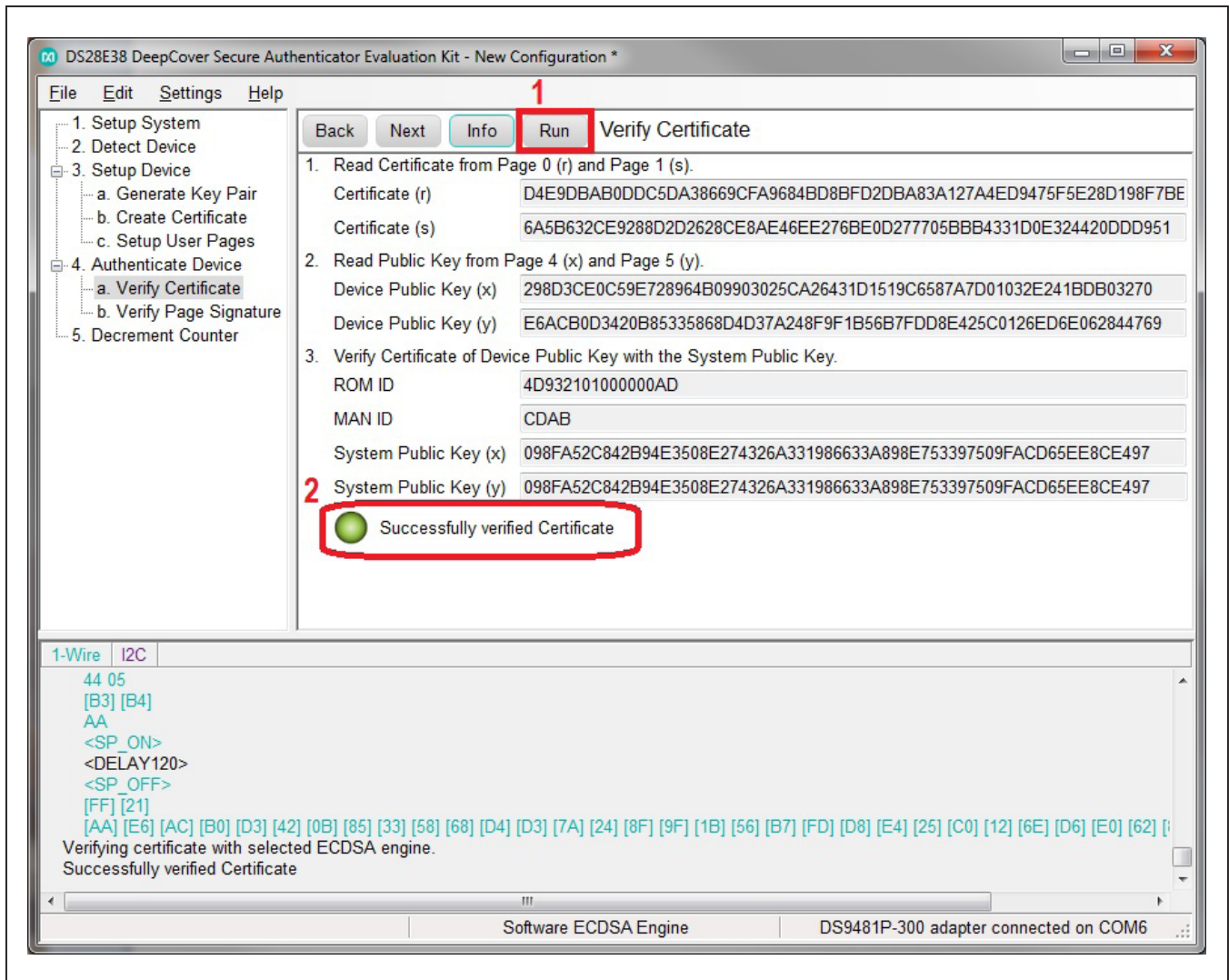


Figure 20. Verify Certificate

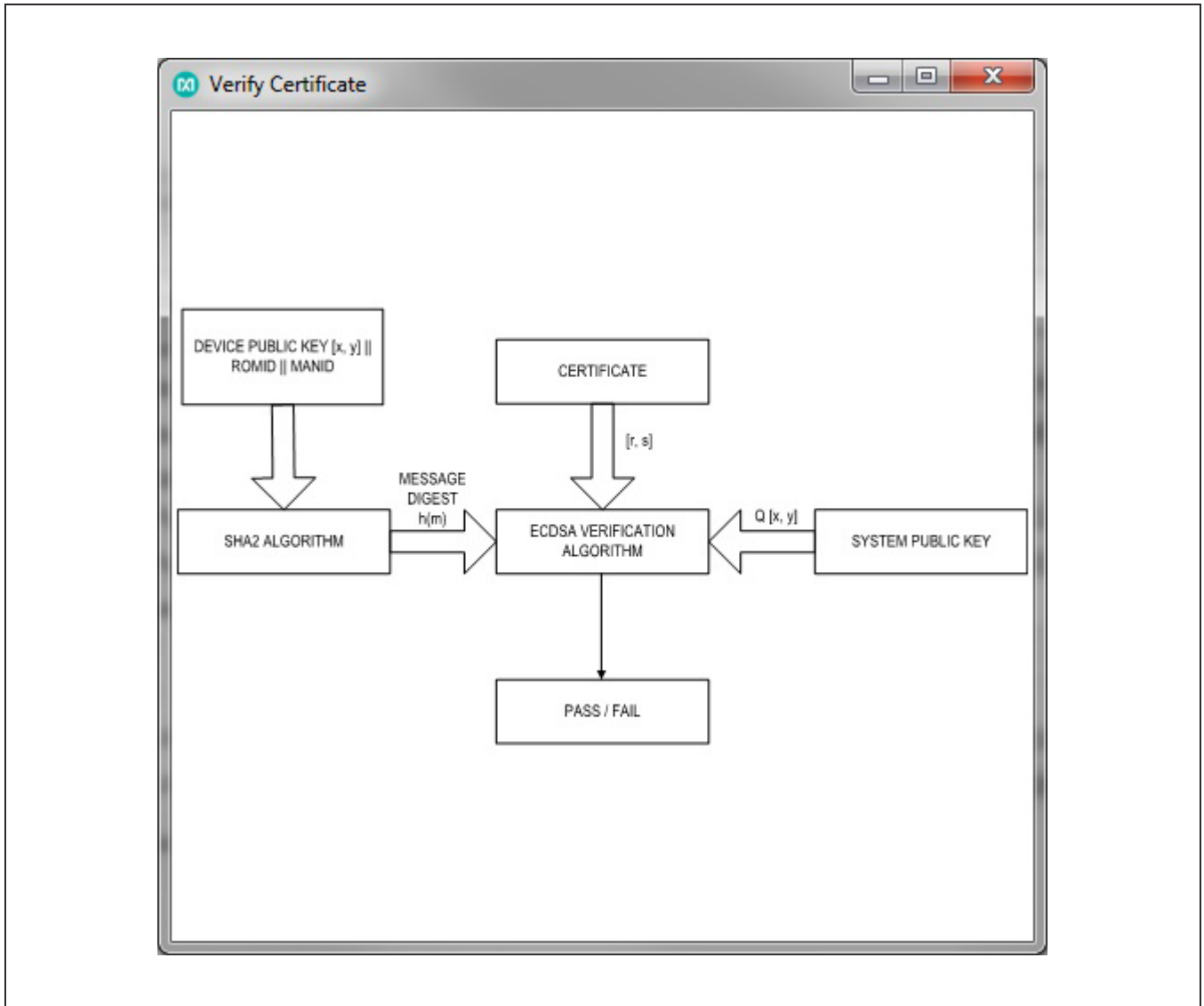


Figure 21. Ingredients Used to Verify the Certificate

b. The host now needs to verify a page signature. Adjust the **Compute authentication signature on Page** field to page 2 where your user data resides. Click on the **Run** button for the host to verify the signature from page 2 of the DS28E38. Confirm the status updated displays **Successfully verified Signature** (Figure 22). During the run process, the host sent a challenge (i.e., generated by the RNG of the host) to the DS28E38 and requested a signature of page 2. The host then reads the signature generated and the page 2 data. Lastly, the host verifies the signature with the device public key. The DS28E38 can now be considered authenticated,

because both its certificate and the signature verified. If only the certificate or only the signature verified, then authenticity could not have been declared because it always requires both to be verified. Click on the **Info** button and a window pops up that shows all the ingredients used in the verification of the signature (Figure 23). The diagram labeled 1 shows the ingredients used by the DS28E38 device to generate the signature. The diagram labeled 2 shows the ingredients used by the host for the verification of the signature. Close the **Verify Certificate** ingredients window and click the **Next** button to proceed to step 5.

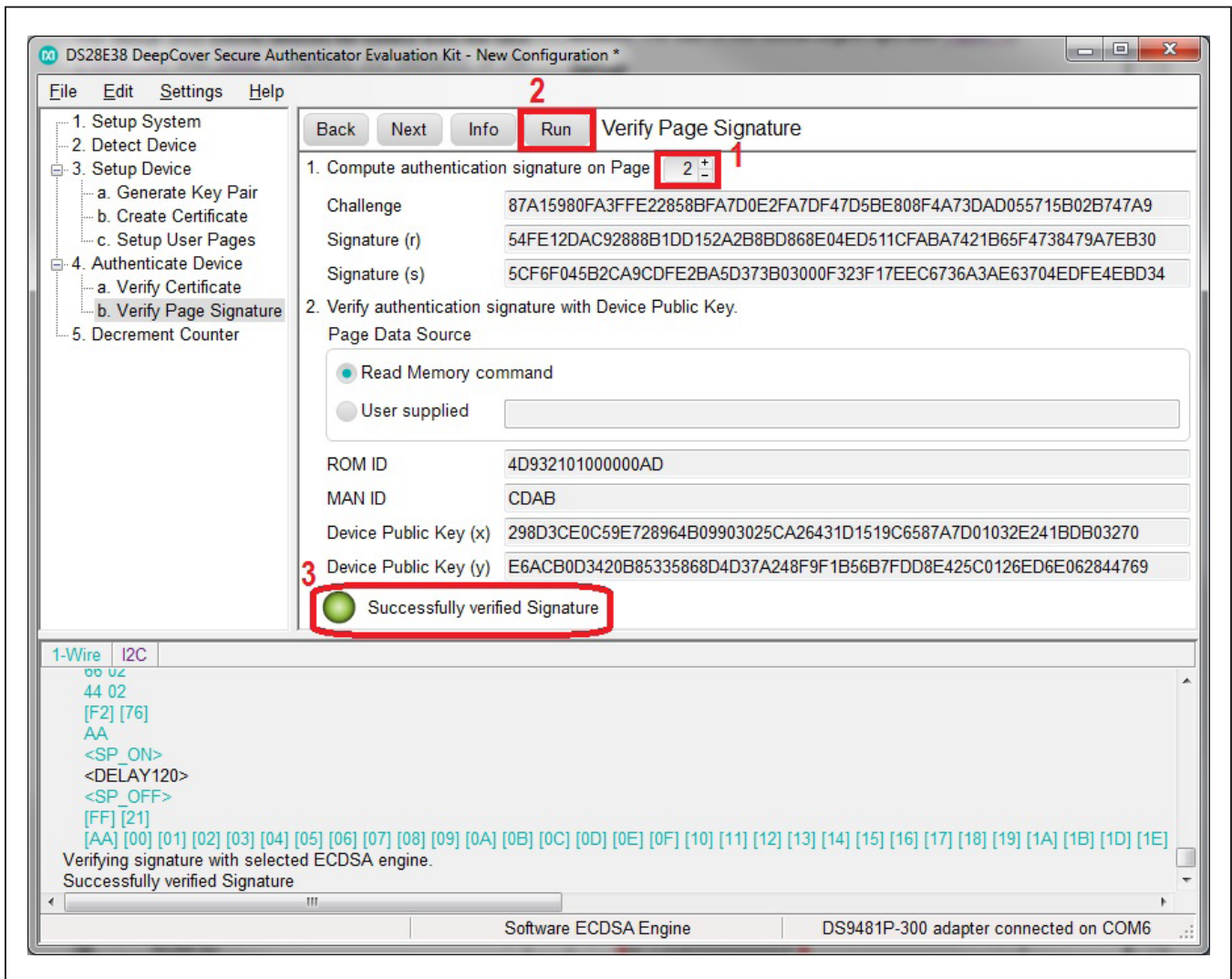


Figure 22. Verify the Signature

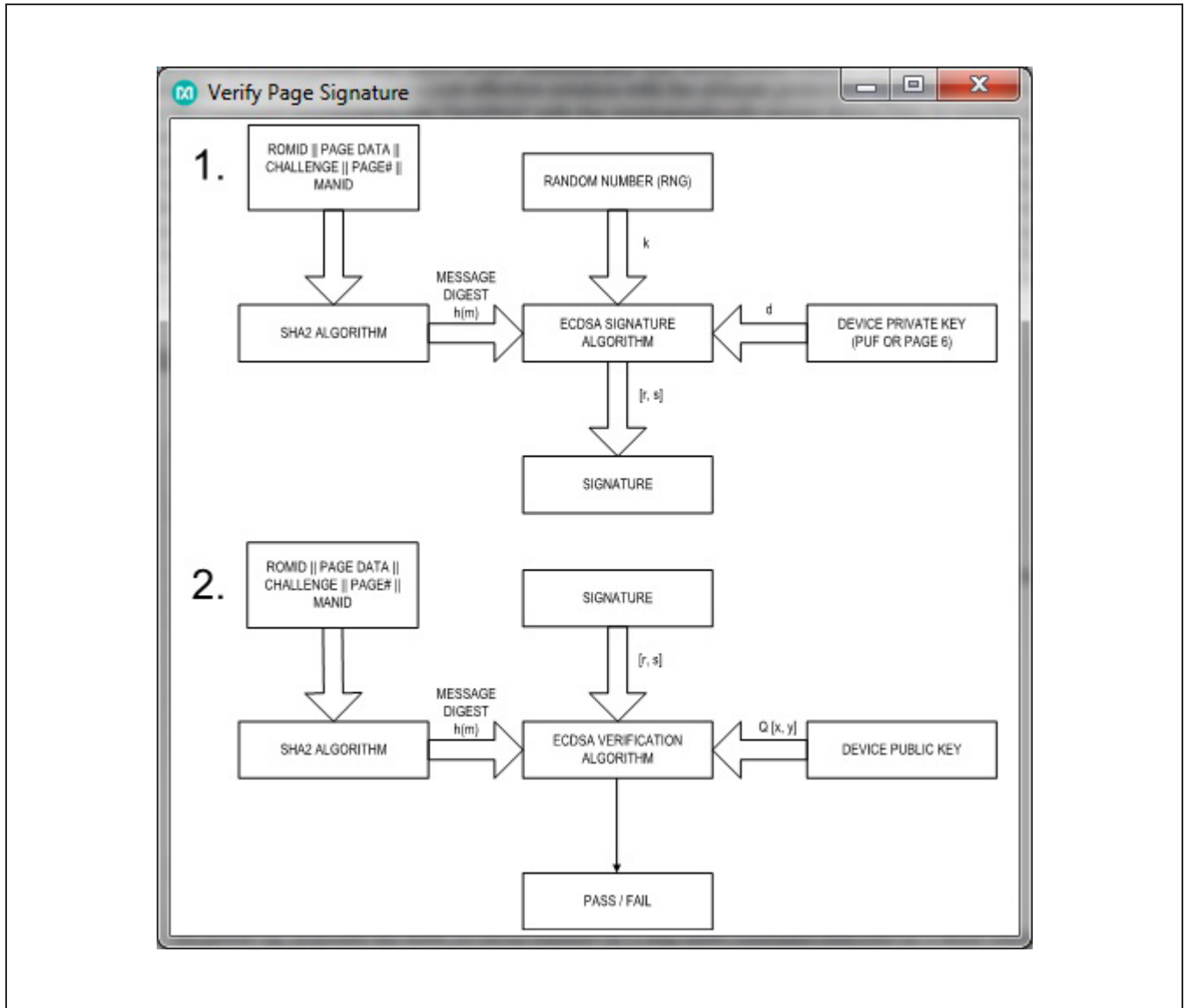


Figure 23. Ingredients Used to Verify the Signature

Step 5: Decrement Counter

Now that the DS28E38 has been determined to be authentic, the decrement counter that was set up on page 3 should be decremented. Click the **Run** button

and confirm the status of the **Counter value** is 131070 (Figure 24). During this run, the host sends the decrement counter command and then reads page 3 to confirm the counter is decremented.

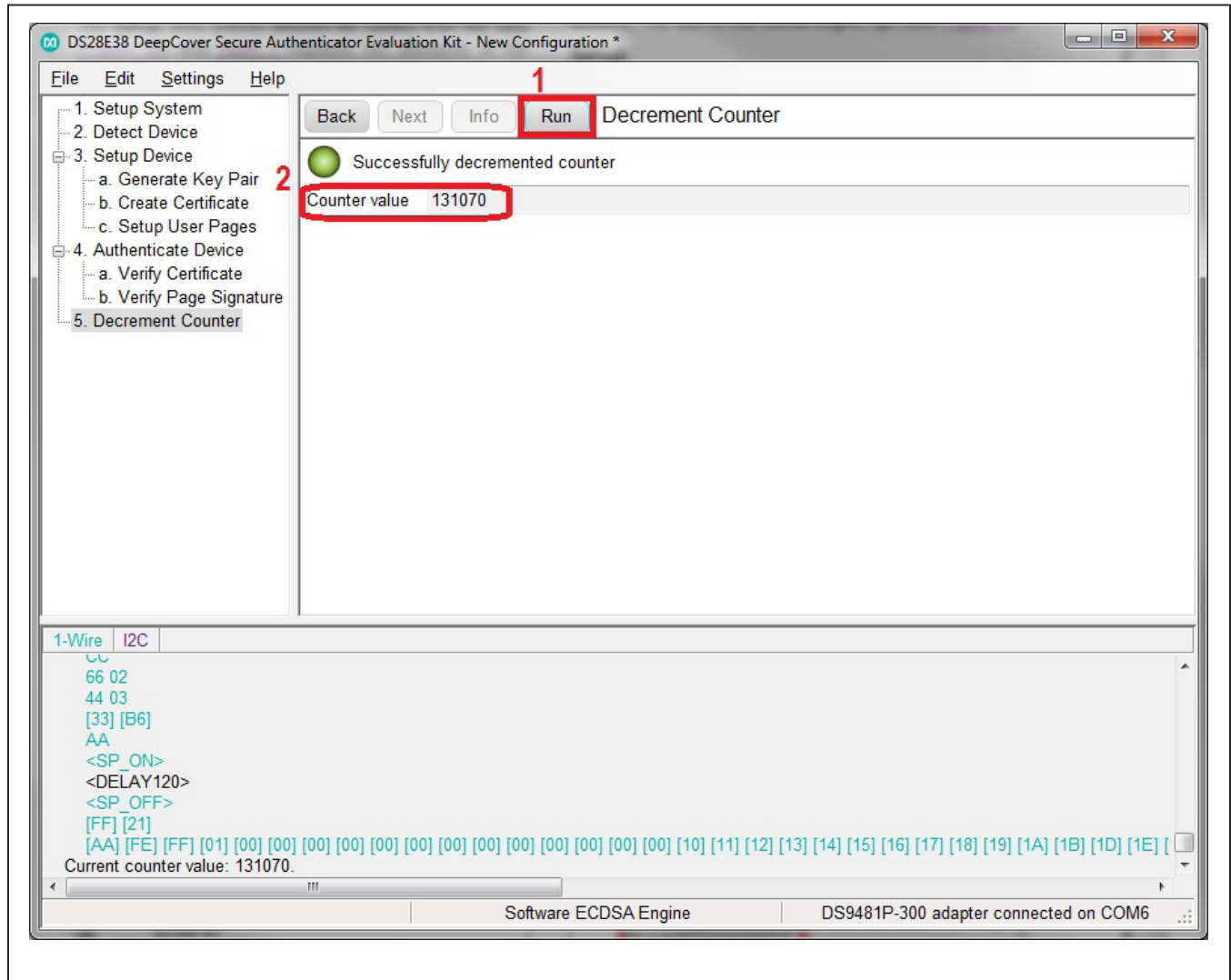


Figure 24. Decrement Counter

Saving the New Configuration

Now that all the steps have been completed successful and authenticated, it is recommended to save the configuration before closing. This allows configuring more DS28E38 devices with the same system key pair. Under

the **File** menu, select **Save As**, give your configuration a name and **Save** (Figure 25). This file contains the system key pair so if this is used in production, then the file needs to be stored in a secure location.

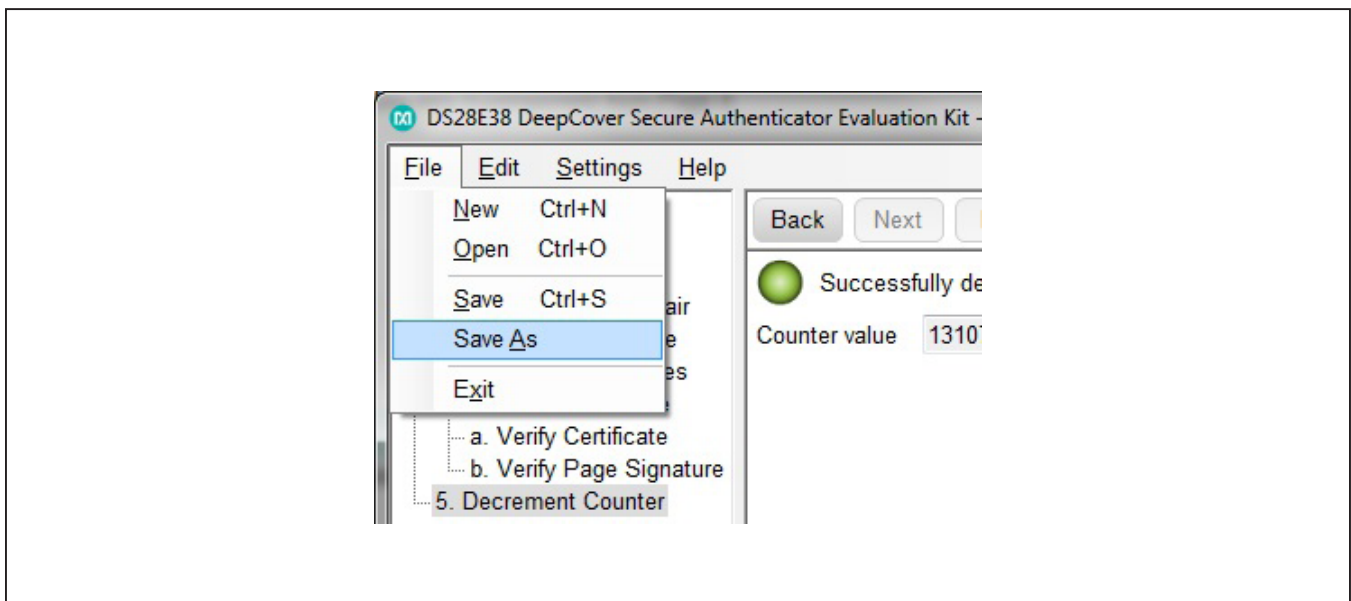


Figure 25. Save As

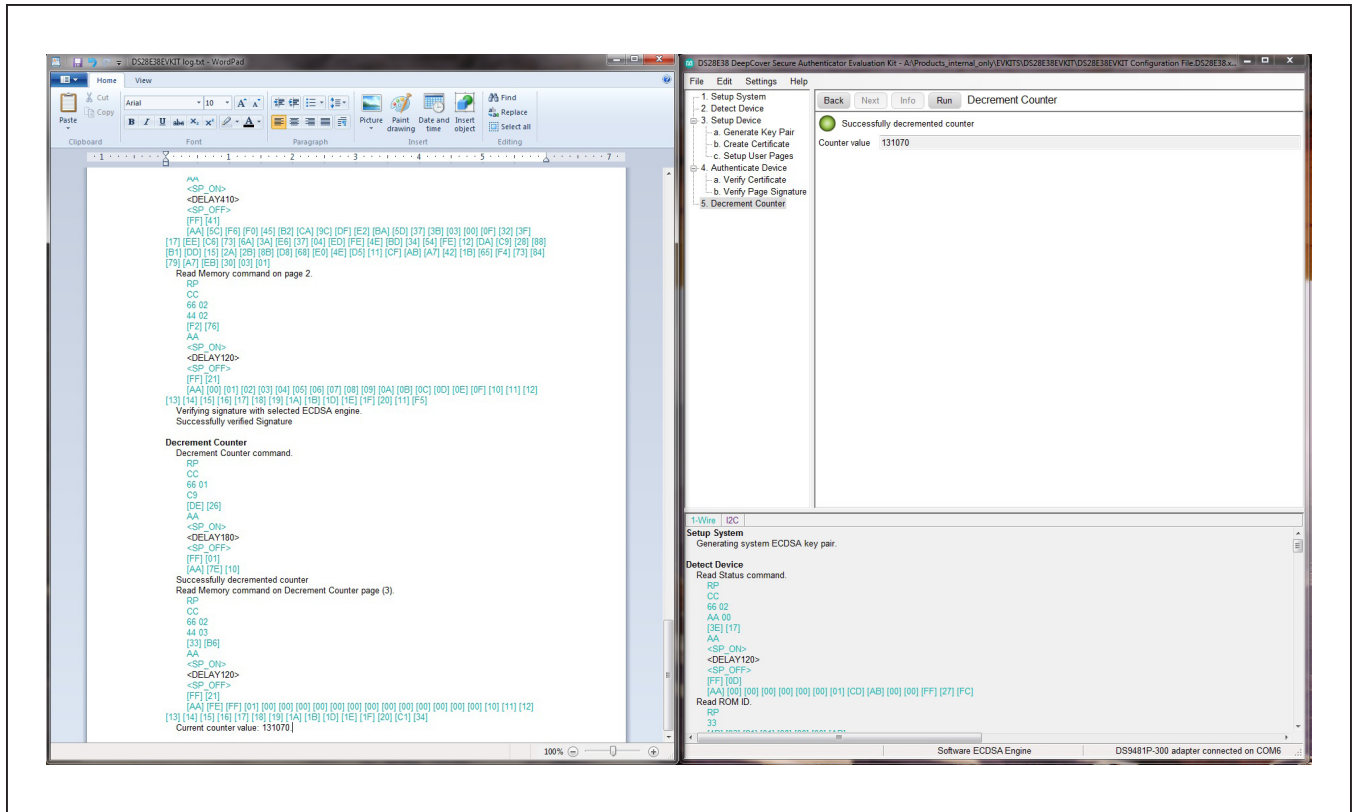


Figure 26. Save the 1-Wire I²C Log

Lastly, to assist the firmware engineer, it is recommended to save the log information, as it shows the 1-Wire sequences for each command. Click on the **1-Wire I²C** log display so the cursor shows, then on your keyboard select all the log text by **Ctrl+A** and copy the log by **Ctrl+C**. Now open a text editor such as WordPad and paste the log with the keyboard by **Ctrl+V** (Figure 26).

Detailed Hardware Description

The DS28E38 EV kit hardware includes the MAXQ1010 microcontroller with USB and two DS9121AQ socket adapters that are made to contain the DS28E38 device or DS2476 device. The MAXQ1010 is loaded with firmware to function as a virtual COM port that bridges UART signaling to I²C and 1-Wire. Optionally, the DS2476 functions to off load the ECDSA computations to perform signature. The DS28E38 1-Wire slave functions to perform ECDSA Public-Key signatures during an authentication and contains memory space for the necessary ingredients.

Ordering Information

PART	TYPE
DS28E38EVKIT#	EV Kit

#Denotes RoHS compliant.

DS9121AQ EV Kit Bill of Materials

DESIGNATOR	QTY	DESCRIPTION	MANUFACTURER	PART NO.
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 1%	Panasonic Electronic Components	ERJ-3EKF1002V
R7, R8	2	RES SMD 10K OHM 1% 1/10W 0603	Panasonic Electronic Components	ERJ-3EKF1002V
C1	1	CAP CER 0.47UF 16V X7R 060	Kemet	C0603C474K4RACTU
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,CLAMHELL,BURNIN	PLASTRONICS	06QN10T23030
JB1, JB2	2	JUMPER BLOCK, .100 2POS VERT,0.318"	Tyco Electronics	22-28-4363
Pack Out	5	DEEPCOVER SECURE COPROCESSOR	Maxim Integrated	DS2476Q+
Pack Out	5	2K EEPROM ECC/SHA2 SECURE AUTHEN	Maxim Integrated	DS28E38Q+
Pack Out	3	SHUNT+,LP W/HANDLE 2 POS 30AU	Tyco Electronics	881545-2

