ANALOG DEVICES

C-Source Reference for Operating the DS28E50 Combined with a DS2477 from a Cortex-M4 Microcontroller

MAXREFDES9008

Introduction

The DS2477 is a 1-Wire[®] master that performs protocol conversion between the I²C master and any attached 1-Wire slaves. For 1-Wire line driving, the internal user-ad-justable timers relieve the system host processor from generating time-critical 1-Wire waveforms, which supports both standard and overdrive communication speeds. The 1-Wire master has a selectable active or passive 1-Wire pullup. The strong pullup features support 1-Wire power delivery for 1-Wire devices that require additional current, such as electrically erasable programmable read-only memory (EEPROM) writes or cryptographic operations.

The DS2477 is also a SHA-3 coprocessor designed to operate with 1-Wire SHA3-256 secure authenticators, such as the DS28E50. The DS28E50 secure authenticator combines FIPS202-compliant secure hash algorithm (SHA-3) challenge and response authentication with Maxim's patented ChipDNA[™] technology, a physically unclonable function (PUF), to provide a cost-effective solution with the ultimate protection against security attacks. The DS28E50 communicates over the single-contact 1-Wire[®] bus at both standard and overdrive speeds.

The MAXREFDES9008 reference design shows how to develop a secure application using a DS28E50 and DS2477 authentication scheme. Featured is an Arm[®] Cortex[®]-M4 host microcontroller to be used as the system's host processor. All hardware design files as well as C-code demonstration software are provided for this reference design in the *Design Resources* Section.

Other features include the following:

- 1-Wire DS28E50 provides SHA3-256 Challenge/ Response Authentication
- DS2477 SHA3-256 Coprocessor stores a system secret securely and performs authentication
- 1-Wire Master DS2477 for Optimized 1-Wire I/O Communication
- Cotex-M4 compatible software libraries for the DS28E50 and DS2477
- C-Code example software to show how to fully authenticate devices

Designed–Built–Tested

A simple, cost-efficient, 1-Wire master and SHA3-256 coprocessor is demonstrated using the DS2477 for a secure authentication application using the MAX32660 host microcontroller and the DS28E50 1-Wire secure authenticator slave. This reference design includes the following major components: one each of MAX32660 Cortex-M4 microcontroller, DS2477 1-Wire master and secure SHA-3 coprocessor, and DS28E50 secure SHA-3 authenticator 1-Wire slave. This document describes the hardware shown in Figure 1 as well as its accompanying software. It provides a detailed, systematic technical guide to set up and understand the MAXREFDES9008 reference design. The system has been built and tested, details of which follow later in this document.



Figure 1. MAXREFDES9008 hardware.

1-Wire and Maxim Integrated are registered trademarks of Analog Devices, Inc. ChipDNA is a trademark of Analog Devices Products, Inc. Arm and Cortex are registered trademarks of Arm Limited.

© 2022 Analog Devices, Inc. All rights reserved. Trademarks and registered trademarks are the property of their respective owners. One Analog Way, Wilmington, MA 01887 U.S.A. | Tel: 781.329.4700 | © 2022 Analog Devices, Inc. All rights reserved.

Quick Start

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

Required Equipment

- 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
- Low-power Arm Micro Toolchain (Windows)
- C-Demo software

- DS28E50 EV Kit
- DS2477 Socket Board
- MAX32660-EVSYS
- Terminal Program such as PuTTY

Procedure

Follow the steps below to set up the demo software:

- 1) Download the ARMCortexToolchain.exe file.
- 2) Double-click on **ARMCortexToolchain.exe** to begin the installation as shown in Figure 2.

File Home Share View					-	
to Quick Copy Paste access	Move Copy to - Copy	New item •	Properties	Select all		
- → × ↑ 🔒 > This PC > Desktop	> install	New Open		v ð	Search install	
Projects 🖈 ^ Name	^	Date modified	Type Size	e		
Projects 🖈 🙆 ARM	CortexToolchain.exe	10/6/2020 10:35 AM	Application	19,505 KB		
kivy-examples *						
Applications *						
Library x						
Document Files						
- Contraction of the second						
Hurwei						
Huawei MAXREFDES9002						
Huawei MAXREFDES9002 Temporary SVN files						
Huawei MAXREFDES9002 Temporary SVN files OneDrive - maximintegr						
Huawei MAXREFDES9002 Temporary SVN files OneDrive - maximintegr						
Huawei MAXREFDES9002 Temporary SVN files OneDrive - maximintegr OneDrive - Personal						
Huawei MAXREFDES9002 Temporary SVN files OneDrive - maximintegr OneDrive - Personal This PC						
Huawei MAXREFDES9002 Temporary SVN files OneDrive - Personal This PC Naturation Y						_

Figure 2. File viewer.

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

- 3) Follow the prompts in the setup wizard to finish the installation as shown in Figure 3.
- 4) Navigate to the toolchain's install directory, open the **Eclipse** folder, and run Eclipse.bat to launch the Eclipse IDE as shown in Figure 4.

Settings	Welcome to the ARM Cortex Toolchain Setup Wizard.	Setup - ARM Cortex Toolchain	🔯 ARM Cortex Toolchain Setup	
Next				
Quit				?
:				×

Figure 3. Toolchain setup wizard.

File Home Share V	Application Tools Eclipse				-	
	t py path te shortcut Vote Copy to Copy Organize	New folder	Properties Den Open	Select all		
← → × ↑ 📑 → This PC	> Windows (C:) > Maxim > Eclipse >			v 0	Search Eclipse	, p
MAXREFDES9002	Name	Date modified	Type Si	ze		
Temporary SVN files	configuration	11/16/2020 11:37	File folder			
OneDrive - maximinteor	dropins	5/10/2019 2:09 PM	File folder			
- oneone maximized	eclipse_neon_updates	5/10/2019 2:07 PM	File folder			
 OneDrive - Personal 	embsysregview	5/10/2019 2:07 PM	File folder			
This PC	features	9/13/2019 3:17 PM	File folder			
3D Objects	gnuarmeclipse_updates	5/10/2019 2:09 PM	File folder			
Desites	🔜 jre	5/10/2019 2:08 PM	File folder			
Desktop	maximProject_updates	5/10/2019 2:09 PM	File folder			
Documents	p2	11/16/2020 11:38	File folder			
Downloads	plugins	9/13/2019 3:17 PM	File folder			
h Music	readme	9/13/2019 3:17 PM	File folder			
E Pictures	eclipseproduct	1/3/2017 2:14 PM	ECLIPSEPRODUCT	1 KB		
Videos	artifacts.xml	9/13/2019 3:17 PM	XML Document	214 KB		
S Mindaws (C)	eclipse.bat	5/15/2018 2:57 PM	Windows Batch File	1 KB		

Figure 4. Eclipse launch location.

- 5) Create a workspace in a desired location as shown in Figure 5.
- 6) <u>Download</u> and extract the **MAXREFDES9008_Soft**ware_V1.0.0 file, in any location as shown in Figure 6.

Eclipse Launcher	×				
Select a directory as workspace					
Eclipse uses the workspace directory to store its preferences and development artifacts.					
Workspace: C:\Users\irvin.salais\Desktop\workspace					
Recent Workspaces					
Copy Settings					
OK Cance	1				

Figure 5. Eclipse workspace creation.

i i i i i i i i i i i i i i i i i i i	Extract View Compressed Folder Tools	Install		-	□ × ~ (
\leftarrow \rightarrow \checkmark \uparrow \square \rightarrow This PC	> Desktop > Install			✓ Õ	
🕂 Downloads 🖈 ^ N	lame ^	Date modified	Туре	Size	
🔮 Documents 🖈	MAXREFDES9008_Software_V1.0.0.zip	9/30/2021 4:37 PM	Compressed (zipp	11.150 KB	
Projects 🖈				Open	
Projects 🖈				Open in new window	
📙 kivy-example 🖈				Share with Skype	
🔒 Applications 🖈				Extract All	
📙 Library 🛛 🖈				7-Zip	
opp_note				CRC SHA	
Career Resource				Pin to Start	
ocs 🖉				📸 TortoiseSVN >	
Final				Edit with Notepad++	
OneDrive - maxim				Scan with Microsoft Defender	
				🖻 Share	
OneDrive - Persor				Open with >	
💻 This PC				Give access to	
🗊 3D Objects				Restore previous versions	
Desktop					
🖾 Documento 🗸 🗸				Send to >	
1 item 1 item selected 10.8 N	1B			Cut	

Figure 6. C-Demo extraction.

7) Open the **MAXREFDES9008_Software_V1.0.0** folder and copy the **demos** and **libraries** folder into the workspace location as shown in Figure 7.



Figure 7. Software workspace.

File	Edit Source Refactor Navigate	Search Project	Run Winde	ow Help	1 m -			4		
	New	Alt+Shift+N >	🎋 🕇 🚺 🕇	8 - 4 -					·	
5	Open Projects from File System							Quic	k Access	B EC
	Class	Ctol v W						🗄 O 🖾	» ₂	
	Close All	Ctrl+Shift+W								a ⊂
	close All	0.1.0						An outline	is not available	e.
	Save	Ctrl+S								
	Save As	Ctrl+Shift+S								
	Revert	Curt Smitt S								
-2	Nove	E2								
	Refrech	F2 F5								
2	Convert Line Delimiters To	· · · · · ·								
	Duint	Chelly D								
	Print	Ctri+P								
	Switch Workspace	>								
	Restart									
2	Import									
2	Export									
	Properties	Alt+Enter								
	Exit									
_										
		Problems	🕅 🔎 Tasks	E Console	Properti.	- 8	1777 EmbSys Registers			
						59 ▽	ERROR: Please select a ch	ip using the p	preference pag	
		0 items				θ.	Register		Hex	Bin
		Description		^		Resource				
		<				>	<			>

8) From the Eclipse dialog box > File menu, select the File > Open Projects from File System... as shown in Figure 8.

Figure 8. Eclipse Open Projects.

9) From the **Import Projects from File System or Archive** dialog box, click **Directory...** button and navigate to the **Demos** folder within the workspace location and click **Finish** as shown in Figure 9.

Import Projects from File System or Archive		– 🗆 X
Import Projects from File System or Archive		
This wizard analyzes the content of your folder or archive	file to find projects and import them in the IDE.	
Import source: C:\Users\irvin.salais\Desktop\workspace	e\demos	V Directory Archive
type filter text		Select All
Folder	Import as	Deselect All
 ✓ demos\DS2477_Exercise ✓ demos\DS28E50_Authentication ✓ demos\Factory_Setup 	Eclipse project Eclipse project Eclipse project	3 of 4 selected Hide already open projects
Use <u>installed project configurators</u> to: Search for nested projects Detect and configure project natures		
Working Sets		New
Working sets:		 ✓ Select
?	< Back Next >	Finish Cancel

Figure 9. Eclipse Open Projects.

10) From the **Putty Configuration** dialog box, open up a terminal and connect it to the MAX32660's corresponding serial COM port as shown in Figure 10.

Figure 10. Opening a serial console.

11) From the **Eclipse** dialog box, select the example program to run under the drop-down box located next to the green **Run** button as shown in Figure 11. The output appears on the serial console as shown in Figure 12.

workspace - C/C++ - Eclipse		– 🗆 X
File Edit Source Refactor Navigate Se	arch Project Run Window Help	
📑 🕶 🔚 🐚 🥸 🕶 🍕 🕶 📾 🔤 💣 🕶 6	3 • 🖻 • @ • 🕸 • 🖸 • 🚱 • 💁 🧀 🔗	- ₽ ■ ■ ≥ 2 + 7 - 4 - 4 -
	1 DS28E50_Authentication	Quick Access 🗄 😭 🗔
	c 2 DS2477_Exercise	
	C 3 Factory_Setup	
E S DS2477 Function	Debug As >	An outline is not available
DS2477_Exercise DS28E50 Authentication	Debug Configurations	An outline is not available.
> 🖾 Factory_Setup	Organize Favorites	
		1
	Problems All lasks Console 🐹 📋 Properti	Embsys Registers 23 Bebugger Console
		Register
	(38) d15 (/64): 0x00000000000000000000000000000000000	A FIEX DIN
	(39) fpscr (/32): 0x00000000	
	===== Cortex-M DWT registers	
	4	
	C	

Figure 11. Running the demo program.

```
Putty COM11 - Putty
                                                                     Х
                                                                DS28E50 Multidrop 1-Wire example using DS2477
                                                                       ~
        *************************
Initializing DS2477's true I2C address...
Fetching DS2477 ROM ID...
Verifying ROM ID CRC8...
Setting up 1-Wire Master timings to default...
Setting up 1-Wire Master speed to Standard...
Setting up 1-Wire Master pull up values to default...
Checking 1-Wire line stability...
Successfully initialized DS2477
Press ENTER to start demo
Populating DS28E50's true 1-Wire ROM ID...
Searching for a DS28E50 ROM ID...
Fetching DS28E50 MAN ID...
Verifying ROM ID CRC8...
Successfully initialized DS28E50
Set device to overdrive speed? (Enter y for overdrive or n for standard)
Setting to standard speed...
Searching for all DS28E50 ROM IDs on 1-Wire bus...
Found 1 devices on the 1-Wire bus:
Device 0 romid:05 0F 56 38 00 00 00 B0
Which device do want to select? (for example enter 0 to select device 0)
Which page do you want to read or write to?
(for example enter r,l to read page 1 or w,l to write to page 1)
Note: only pages 0 - 5 are available for this demo
r,0
[AA] [AA] [AA]
Do you want to quit (y or n)?
```

Figure 12. Console output for the demo program.

Detailed Description of Hardware

A detailed block diagram of the MAXREFDES9008 hardware is shown in Figure 13. A Maxim Integrated® MAX32660 Cortex M4 microcontroller is used as the system's host controller for the DS2477 through its I2C peripheral. The MAX32660's I2C port pins, P0_8 and P0_9, are connected to the DS2477's SDA and SCL pins, respectively, each with a 10k Ω external pullup resistor connected to 3.3V. The DS2477 bridges 1-Wire communication to a DS28E50 secure authenticator device by connecting the DS2477's and DS28E50's IO pins together.

Detailed Description of Software

The MAXREFDES9008 software consists of C-code demonstration programs for using the DS2477 and DS28E50 SHA3-256 authentication schemes. For a detailed list of available C-programs, see Table 1. The software is supported on the MAXREFDES9008 hardware and includes the firmware and source files for programming an Arm Cortex-M4 processor-based micro-controller like the MAX32660. This C-Demo software utilizes the DS2477 and DS28E50 APIs for convenient interfacing within the system. The software is compatible

with the Maxim toolchain, that can be found in the <u>Design</u> <u>Resources</u> tab of the MAX32660 and can be directly imported into an Eclipse IDE workspace. For details on how to set up the C-Demo software, see the <u>Quick Start</u> Section.



Figure 13. MAXREFDES9008 detailed block diagram.

Table 1. Demos Overview

DEMO PROGRAM	DESCRIPTION
DS2477_Exercise	Designed to get familiarized with the DS2477 and its 1-Wire master capabilities.
Factory Setup	For programming both the DS28E50 and the DS2477 in preparation for an authentication.
DS28E50_Authentication	For authenticating the DS28E50 target device. Computes unique secret for the DS28E50 1-Wire SHA-3 authenticator device and performs and verifies a Compute and Read Page Authentication on a preprogrammed device page. The DS28E50 and the DS2477 must first be setup with the 'Factory Setup' demo.

DS2477 API

Table 2 shows a brief overview of the DS2477 API. This API allows the MAX32660 to interface with the DS2477 through I^2C and provides access to its commands.

Table 2. DS2477 API Overview

DS28E50 API

The C-Demo software also provides a DS28E50 API. A brief overview of the DS28E50 API is shown in Table 3. This API makes it easy to exercise all the features of the DS28E50.

FUNCTION	DESCRIPTION
DS2477_WriteMemory	DS2477 performs a 'Write Memory' command.
DS2477_ReadMemory	DS2477 performs a 'Read Memory' command.
DS2477_ReadStatus	DS2477 performs a 'Read Status' command.
DS2477_ReadRNG	DS2477 performs a 'Read RNG' command.
DS2477_SetPageProtection	DS2477 performs a 'Set Page Protection' command.
DS2477_EncryptedReadMemory	DS2477 performs a 'Encrypted Read Memory' command.
DS2477_ComputeAndLockSecret	DS2477 performs a 'Compute and Lock Secret' command.
DS2477_ComputeSessionKey	DS2477 performs a 'Compute Session Key' command.
DS2477_ComputeHMAC	DS2477 performs a 'Compute HMAC' command.
DS2477_ComputeSHA3	DS2477 performs a 'Compute SHA3' command.
DS2477_ReadOneWirePortConfig	DS2477 performs a 'Read 1-Wire Port Config' command.
DS2477_WriteOneWirePortConfig	DS2477 performs a 'Write 1-Wire Port Config' command.
DS2477_MasterReset	DS2477 performs a 'Master Reset' command.
DS2477_OneWireCommand	DS2477 performs a '1-Wire Command' command.
DS2477_OneWireBlock	DS2477 performs a '1-Wire Block' command.
DS2477_OneWireWriteBlock	DS2477 performs a '1-Wire Write Block' command.
DS2477_OneWireReadBlock	DS2477 performs a '1-Wire Read Block' command.
DS2477_OneWireSearch	DS2477 performs a '1-Wire Search' command.
DS2477_FullCommandSequence	DS2477 performs a 'Full Command Sequence' command.
DS2477_ComputeCrc16	DS2477 performs a 'Compute CRC16' command.

Table 3. DS28E50 API Overview

FUNCTION	DESCRIPTION
DS28E50_Initialize	Populates the ROM ID for all DS28E50 devices found on the 1-Wire bus.
DS28E50_WriteMemory	DS28E50 performs a 'Write Memory' command.
DS28E50_WriteMemoryEX	DS28E50 performs a 'Write Memory EX' command.
DS28E50_ReadMemory	DS28E50 performs a 'Read Memory' command.
DS28E50_ReadStatus	DS28E50 performs a 'Read Status' command.
DS28E50_SetPageProtection	DS28E50 performs a 'Set Page Protection' command.
DS28E50_ReadRNG	DS28E50 performs a 'Read RNG' command.
DS28E50_EncryptedReadMemory	DS28E50 performs a 'Encrypted Read Memory' command.
${\tt DS28E50_ComputeAndReadPageAuthentication}$	DS28E50 performs a 'Compute and Read Page Authentication' command.
DS28E50_AuthenticatedWriteMemory	DS28E50 performs a 'Authenticated Write Memory' command.
DS28E50_ComputeAndLockSecret	DS28E50 performs a 'Compute and Lock Secret' command.
DS28E50_DecrementCounter	DS28E50 performs a 'Decrement Counter' command.
DS28E50_Device_Disable	DS28E50 performs a 'Device Disable' command.

Design Resources

Download the complete set of **Design Resources** including the schematics, bill of materials, PCB layout, and C-demo software.

Revision History

REVISION	REVISION	DESCRIPTION	PAGES
NUMBER	DATE		CHANGED
0	2/22	Initial release	



www.analog.com

Information furnished by Analog Devices is believed to be accurate and reliable. However, no responsibility is assumed by Analog Devices for its use, nor for any infringements of patents or other rights of third parties that may result from its use. Specifications subject to change without notice. No license is granted by implication or otherwise under any patent or patent rights of Analog Devices. Trademarks and registered trademarks are the property of their respective owners.